
المجاهد التقني
مجلة دورية تصدر عن مركز الفجر للإعلام
العدد الثاني لشهر صفر، سنة ١٤٢٨ هجرية
٢
كيف تخفي معلوماتك داخل صورك
سلسلة شرح الفيديو [ج٢]
ترجمة الأفلام عن طريق العناوين الجانبية
كيف تنشئ موقعا جهاديا من الألف الى الياء [ج١]
برنامج أسرار المجاهدين رؤية من الداخل
الأسلحة الذكية : صواريخ أرض جو
مركز الفجر للإعلام
الفجر



لماذا مجلة المجاهد التقني؟

إن مجلة المجاهد التقني تُعنى بكل ما يفيد المجاهد في الجانب الإعلامي من جهة ورواد المنتديات الجهادية من جهة أخرى. فالمجلة تهتم بمتابعة الجديد والمفيد في أمن المعلومات وطرق حماية الحواسيب والمونتاج والهندسة الصوتية وأخبار الجهاد الإعلامي ورصدٍ لأقاويل قادة الصليبيين حول أثر الجهاد الإعلامي عليهم ونحو ذلك .

والأهداف التي نسعى إلى تحقيقها بإصدار المجلة هي :

1- نزع عقدة الخوف والهلع الموجودة في نفوس البعض والتي تحجزهم عن المشاركة بشكلٍ فاعلٍ في خدمة الجهاد لكون أحدهم يظن أن المخابرات يعدّون عليه أنفاسه وحركاته، فيعرّف بواقع الحال وبمبالغته فيعرف متى يقدم ومتى يحجم.

2- نشر الحس الأمني بشكل علمي لدى أعضاء المنتديات الجهادية من باب أخذ الحذر الذي أُمِرنا به بطريقة منطقية مرتبة وواقعية وبدون مبالغة أو تهوين.

3- نشر الوعي التقني بكل ما يفيد في مجال الإعلام الجهادي في مجال المونتاج المرئي والهندسة الصوتية وغيرها من أساسيات الإعلام.

4- نشر مقالاتٍ علمية عن بعض التقنيات الحديثة التي من شأنها تطوير عمل الإخوة المجاهدين في الميدان

فريق العمل

رئيس التحرير: أبو المثنى النجدي

الكتاب المشاركون في العدد: أبو مصعب الجزائري، أبو الحسن المغربي، أبو دجانة المكي، أبو الحارث الدليمي، مجاهد إعلامي.

تدقيق و مراجعة : أبو محمد المراكشي

الإخراج الفني : أبو الزبير المدني

تقرؤون في هذا العدد:

الكلمة الافتتاحية

بسم الله الرحمن الرحيم

الحمد لله رب العالمين, والصلاة والسلام على إمام المجاهدين, نبينا محمد وعلى آله وصحبه أجمعين, أما بعد.....

فها نحن نعود إليكم من جديد في هذا العدد من مجلتنا المباركة بحول الله .

في البداية نود أن نشكر و نثمن بشدة أولئك الإخوة الذين شجعونا وأيدونا ولم يبخلوا علينا بآرائهم وملاحظاتهم وأسئلتهم حول المجلة وعددها الأول.

وإن كنا قد بدأنا بالشكر فلا ننسى إخوتنا الذين استجابوا لدعوتنا وأرسلوا لنا مقالاتهم التقنية لنشرها في المجلة ونقول لهم إن كان الوقت لم يسعفنا هذه المرة والمجلة لم تتسع للكل في هذا العدد فإننا نعدكم أن مقالاتكم ستظهر في الأعداد القادمة للمجلة بإذن الله تعالى. وإننا لننتهز هذه الفرصة لنشد على أيدي باقي إخوتنا للبدء بالعمل والإبداع وإرسال مقالاتهم أو اقتراحاتهم إلينا .

بقي أن نذكر أننا لم نتمكن من الرد على جميع الإخوة الذين راسلونا باقتراحات أو طلبات ولكن نود أن نعلمهم أن كل ما كتبوه سيؤخذ في الاعتبار بحول الله .

بالنسبة لهذا العدد سيتم طرح عدة مواضيع متنوعة ابتداء بمسائل الفيديو و المونتاج حيث أنها مسائل محورية للعمل الإعلامي الجهادي. أيضا هذا العدد يحتوي على مقالات مهمة في حماية المعلومات سواء بتشفيرها أو بإخفائها في أشكال صور إلكترونية. كما أننا قررنا في هذا العدد البدء بسلسلة تشرح خطوات إنشاء استضافة وافتتاح موقع للأغراض الجهادية على الإنترنت.

وإننا ماضون في حربنا هذه مع أعداء الله فوق كل أرض وتحت كل سماء حتى تحرر جميع أراضي المسلمين من رجس اليهود المعتدين والصليبيين الحاقدين ويكون الدين كله لله ونرى راية الإسلام خفاقة في الأرض.

والله أكبر والعزة لله ولرسوله وللمؤمنين....

يسعدنا تلقي استفساراتكم ورسائلكم على بريد المجلة
http://teqanymag.arabform.com

أخوكم / رئيس التحرير
أبو المثنى النجدي



الإتصالات السرية: إخفاء الأسرار داخل الصور

بقلم: أبو مصعب الجزائري



أكثر شيء يخيف مكتب التحقيقات الفدرالي الأمريكي هو استخدام المجاهدين لتقنيات الاتصالات السرية المعروفة بعلم الإخفاء.

علم الإخفاء (Steganography) أو إخفاء المعلومات (Information Hiding) هو أحدث تقنية في النقل الآمن للمعلومات سواء كان ذلك عبر شبكة الانترنت، شبكة الهاتف النقال ... أو غير ذلك من وسائط نقل المعلومات.

وبينما يمثل علم تشفير البيانات باستخدام خوارزمية المفتاح العام ضماناً لسرِّية المعلومة وأمن البيانات الخاصة، فإن نقطة الضعف في التشفير هو معرفة الآخر أنك تقوم بنقل معلومات مشفرة، و هذا في حد ذاته يشكل نوعاً من الخطر على مرسل البيانات المشفَّرة ويدفع الكثير من الأجهزة إلى متابعة الشخص المرسل نفسه ومعرفة مصدر الارسال. وهنا يتدخل علم إخفاء المعلومات، فهو يلغي نقطة ضعف علم التشفير بحيث يقوم بإخفاء المعلومات المشفرة بجميع أنواعها داخل بيانات أخرى مثل الصور والمقاطع الموسيقية أو غيرها.

هذه الدراسة وظيفتها التعريف بتقنية إخفاء المعلومات وتقنية كشف المعلومات الخفية –أو ما يعرف باسم "تحليل الإخفاء"–، كما سنحذر من عدد من البرامج التي تدَّعي إخفاءها للمعلومات بينما هي في حقيقتها برامج مخادعة لا يجب أن يستخدمها أحد لأن ضررها فادح، فبينما تعتقد أنك قد أخفيت معلوماتك باستخدامها فإن استخراج هذه المعلومات يتم ببساطة شديدة. علماً أن الصورة أعلاه توضيحية فقط وعملية الإخفاء تختلف جذرياً عما يظهر هنا.

مع انتشار تقنيات الوسائط المتعددة بدايةً من 1990 بدأ الاهتمام بإخفاء المعلومات داخل الوسائط الرقمية. بدايةُ هذه التقنية كانت قد سبقتها العلامات المائية (Watermarking) لحماية حقوق التأليف في الوسائط المتعددة مثل الصور والحفاظ على حقوق أصحابها. الهدف الحقيقي هو نقل معلومات سِرِّية داخل غطاء من الوسائط الرقمية بعيداً عن أية شبهة وبالتالي تفادي اعتراض هذه البيانات أو حتى العلم أن هناك نقلاً للمعلومات.

الاهتمام بإخفاء المعلومات جاء من قبل الباحثين في مجال معالجة الإشارة والصور الرقمية كنوعٍ جيِّد من تقنيات أمن المعلومات، وكشفت هذه التقنيات عن تخوف الكثير من الدول من استخدام هذه التقنية في نقل معلوماتٍ تضرُّ بالأمن العام وبمصالح الدول. وبدأ بعد



ظهور هذا التخوُّفِ مجالٌ جديدٌ من البحث في الطرق المضادة التي تكشف إمكانية وجود معلومات مخفية داخل الوسائط الرقمية، وسُمِّي هذا المجالُ من البحث بتحليل الإخفاء (Steganalysis).

وتكمن قوة تحليل الإخفاء في ضعف تقنيات الإخفاء، فبينما يتمكن علم تحليل الإخفاء من كشف بعض الوسائط الرقمية الحاملة لمعلوماتٍ خفيَّة، فإنه يفشل تماماً في الكثير منها بسبب تطور خوارزميات الإخفاء، خاصةً أن الوسائط الرقمية تعد بمئات الملايين من الصور المنتشرة عبر شبكة الإنترنت ويستحيل تحليل هذا الكم الخرافي.



رسم 2. صورة ملونة مع صور الألوان الأساسية المكونة لها (RGB). الصورة الأساسية هي صور من السلم الرمادي (Grayscale) مكونة من 256 لون لكل واحدة منها و عند دمجها مع بعض تنتج الصورة الملونة.

1. تقنيات حديثة و تاريخ قديم:

ارتبط إخفاء المعلومات قديما بالتجسس على العدو ومحاولة نقل أسرارٍ من دون التعرُّضِ للكشف. والحبر السِّرِّيُّ كان أحـــدها، والذي اعتمد على سائل البصل قديماً قبل أن يتطور في خمسينيات وستينيات القرن الماضي على يد رجال الهندسة الكيميائية الذين اخترعوا سوائل حديثة للكتابة بها بين الأسطر. يكتب الجاسوس رسالة عادية لصديق وبين الأسطر يستخدم الحبر السري في كتابة معلومات ســـرية.



فالرسالة الظاهرة هي وسيط النقل بينما الرسالة الحقيقية هي في الواقع ما لا يراه القارئ. ويتم استخراج النص السري عن طريق مسح الرسالة الورقية بمادة كيميائية خاصة تتفاعل مع المادة الخفية مما يظهر النص السري.

وربما يذكر الكثير قصة رجل الاستخبارات المصري رفعت الجمان (رأفت الهجان) الذي جنّدته الاستخبارات المصرية تحت اسم شاب يهودي لتزرعه في داخل الكيان الصهيوني في فلسطين المحتلة، وكان قد تم تدريبه في البداية ليقوم بنقل المراسلات السرية عبر كتابة رسائل لصديقته في باريس. وصديقته لم تكن سوى شقة للاستخبارات المصرية في فرنسا. وبعد تطور هندسة الاتصالات تدرب رأفت أو رفعت على إرسال واستقبال الرسائل المشفرة عبر اللاسلكي باستخدام شيفرة مورس، وكانت هذه اللغة التي اخترعها العالم مورس أول ظهور للإرسال الرقمي اللاسلكي في 1890 لأنها كانت تعتمد على ترميز الحروف باستخدام حالتين فقط (Mark and Space)، وهو ما عرف بعد ذلك باللغة الثنائية في الاتصالات الرقمية (Binary encoding in Digital Communication).

2. إخفاء المعلومات (Information Hiding):

بينما يهتم علم التشفير في حماية سرية المعلومات ومنع أي شخص من الاطلاع على محتوى الرسائل المشفرة، فإن علم الإخفاء يذهب بعيداً في تأمين سرِّية نقل المعلومات نفسها. فالتشفير ينقل المعلومات ولا يهتم بأن يعرف الآخرون أن هناك اتصالاتٍ مشفرة، بينما علم الإخفاء وظيفته نقل المعلومات دون أن يعرف شخص ما أن هناك أي اتصال. وعلم الإخفاء ينقل المعلومات السرية داخل الوسائط المتعددة بعد أن يقوم بتشفيرها بخوارزميات عالية الأمان تستخدم مفاتيح يتراوح طولها بين 256 بت و 2048 بت.

وظيفة الإخفاء هو نقل المعلومات السرية دون أن تكون هناك أدنى شكوك حول تبادل رسائل، تحت غطاء وسائط رقمية بريئة من أية شبهة. الصور هي أكثر وسيط أو غطاء في نقل الرسائل الخفية، وقد تم استخدام صور من النوع من دون ضغط (Bitmap) ومن النوع المضغوط (Jpeg)، ويتم إخفاء المعلومات داخل الصور الملونة اعتماداً على عدة طرق منها تغيير البت ذي الدلالة الصغرى ومنها طرق تدخل في المجال الترددي (Frequency Domain).

2.1 تعديل البت ذي الدلالة الصغرى [LSB modification]:

ويتم في هذه التقنية تغيير البت ذي الدلالة الصغرى في لون عنصر الصورة (Pixel)، وهو أصغر بت في اللون وتغييره لا يؤثر مطلقاً على الصورة لأنه يمثل جزءاً من 255 جزء من اللون الأساسي. فالألوان الأساسية في الصور الرقمية هي الأحمر، الأخضر والأزرق، وهذا يعني أنه بإمكاننا استغلال ثلاثة بت (3 bits) من كل عنصر صورة مكون من 24 بت.

وتغيير أصغر بت في اللون يقوم بادخال نوع من التشويش على الصورة يقاس بما يعرف بمعامل الإشارة على الضجيج (Signal to Noise Ratio) و يختصر بـ SNR، وقيمة هذا المعامل في هذه الحالة تعادل 50 ديسيبل (Decibel-dB) مما يعني أن التغيير على الصورة لا يمكن ملاحظته. ولحساب كمية المعلومات التي يمكن إخفاؤها داخل صورة ما نقوم بالعملية التالية:

$$ك = 3.\frac{ط.x.ع}{8}$$



بحيث يكون للاختصارات المعاني التالية:

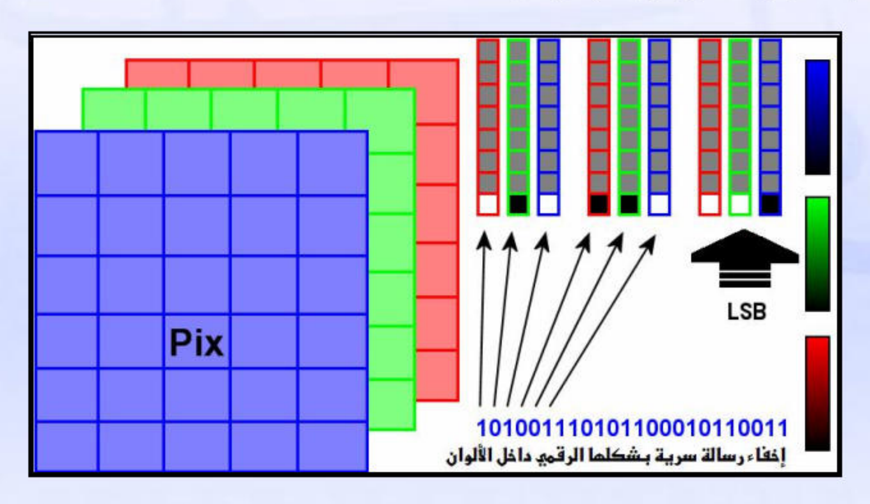
ك: كمية المعلومات المدمجة.

ط: طول الصورة (الحاملة للرسالة الخفية).

ع: عرض الصورة.

علماً أن هذه الكمية للمعلومات قبل إدخال الضغط عليها، فإذا تم استخدام ضغط المعلومات فهذا يعني أن الكمية سوف تكون أكبر بكثير مما حسبناه. وهذا يعني مثلاً أنه من دون ضغط يمكننا إخفاء رسالة مكونة من 300 حرف في صورة بعرض 800 بكسل و بارتفاع بكسل واحد، ومثل هذه الصورة لا يتم الانتباه لوجودها أصلاً في أي موقع الكتروني وتكون من ضمن تصميم الموقع نفسه ولا تثير أية شبهة. طبعاً عند ضغط الرسالة يمكننا إخفاء كمية أكبر قد تصل إلى أضعاف الكمية التي قمنا بحسابها.

و من البرامج الشهيرة التي تقوم بدمج الرسائل أو المعلومات بهذه الطريقة نذكر على سبيل المثال لا الحصر: EzStego, S-Tools, Hide and Seek. لكن يجب أن نفرق بين إخفاء المعلومات في صور لا تخضع للضغط والصور التي تخضع للضغط، حيث أن الضغط يقوم بتغيير قيم الألوان حسب اختيار نوعية الصورة (image quality).



رسم 3. الثلاث طبقات التي تكون الصور الملونة و توضيح البت ذي الدلالة الصغرى (LSB) في كل لون أساسي. حيث أن كل لون أساسي مكون من ثمانية بت. ويتم إدخال 3 بت في كل بكسل.

تمثل عبارة Pix عنصر الصورة ويمثل LSB البت ذي الدلالة الصغرى. وتبين هذه الصورة أن الصور الملونة مكونة من ثلاث طبقات هي عبارة عن الألوان الرئيسية (أحمر، أخضر، وأزرق). وكل لونٍ مكون من ثمانية بت وبذلك يمكنه ترميز 256 مستوى من اللون الأساسي، وهذا يعني أن كل عنصر صورة مكون من 24 بت، وهو ما يمثل 16,777,216 لون.



يتم استغلال ثلاثة بت من كل عنصر صورة لهدف دمج وإخفاء الرسائل أو المعلومات السرية، علماً أن دمج هذه المعلومات لا يؤثر لا على حجم الصورة ولا على نوعيتها، ويبدو وكأن شيئاً لم يتغير. وبخلاف ذلك، لا تعتبر التقنية إخفاءً حقيقياً كما سوف نرى لاحقاً في بعض البرامج التي تسوَّق على أنها برامج إخفاء بينما هي في الواقع تختلف كلياً عن ذلك ويتم كشف المعلومات المخفية في داخلها بسهولة بالغة.

3. البصمة الرقمية:

البصمة الرقمية عبارة عن شيفرة تتراوح في طولها بين 128 بت و512 بت يتم عن طريقها التأكد من أن ملفاً ما هو النسخة الأصلية ولم يتم التلاعب به، وكذلك تستخدم هذه البصمة في حفظ كلمة السر داخل الملفات. وتقنية البصمة مبنية على خوارزمية تشفير أحادية الاتجاه (one way encryption)، وهذا يعني أنه لا يمكن استرجاع كلمة السر من البصمة وهو يعرف باسم خوارزمية الهاش (Hash) أو هضم الرسالة (Message Digest).



رسم 4. برنامج لحساب البصمة الرقمية للنصوص أو الملفات – البصمة هي تحويل أحادي الإتجاه.

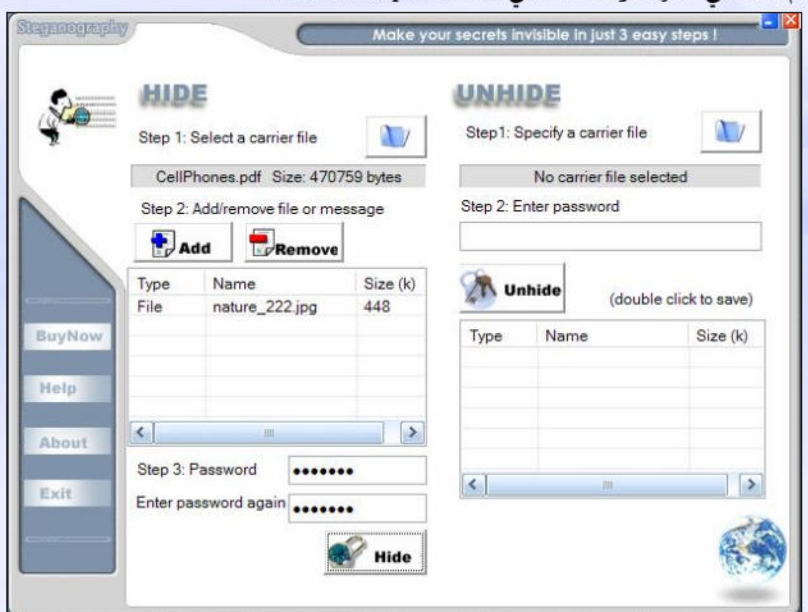
4. تحليل الإخفاء أو الحلول المضادة (Steganalysis):

علم تحليل الإخفاء جاء ليقوم بالدور العكسي لما يقوم به علم الإخفاء، فوظيفة تحليل الإخفاء هو كشف ما إذا كان وسيطٌ معين (صورة، صوت أو غير ذلك) يخفي معلومات سرية. والتحليل يعتمد على نوع الوسيط، فإذا كان الشك يدور حول صورة معينة فإن تقنيات معالجة الصور الرقمية هي التي يتم اللجوء إليها في تحليل طبقات (LSB).



فالصورة الملونة تحتوي على 24 بت منها 3 بت (بت واحد من كل لون أساسي) يدور حولها الشك في إخفاء المعلومات، يتم استخراج هذه الثلاث طبقات وملاحظة ما إذا كانت هناك اختلافات من الناحية الإحصائية (Statistical analysis) في عموم مناطق الصورة. طبعاً هذه التقنية تفشل تماماً إذا تم تشفير المعلومات قبل إخفائها وتوزيعها بطريقة مناسبة داخل الصورة.
ومن الصور التي يسهل فيها كشف الإخفاء هي الصور المضغوطة من نوع JPG لأن الألوان مرتبطة مع بعض عن طريق (DCT (Discrete Cosine Transform) وأي تعديل في الألوان عن طريق إخفاء معلومات معينة داخل الصورة يسبب خللاً في معاملات DCT) (coefficients و بالتالي يسهل كشف وجود معلومات خفية حتى لو لم يتم استخراجها. ولتقليل احتمال كشف الرسائل تقوم بعض البرامج باستغلال عددٍ قليلٍ من طبقات الألوان، كأن يتم مثلاً إخفاء الرسالة في طبقة اللون الأحمر فقط.

هناك برامج تباع على شبكة الإنترنت على أساس أنها برامج إخفاء للمعلومات بينما هي في حقيقتها لا تمت بصلةٍ لعلم الإخفاء وإنما تعتمد على التلاعب في تعريف بداية و نهاية الملف. ونعرض في هذه الدراسة أحدث برنامج و يسمى (Steganography 1.8) ونكشف كيف يتم استخراج ما تم إخفاؤه ببساطة شديدة تلغي كل ما يدَّعونه من تشفيرٍ للبيانات التي تم إخفاؤها. بعد فتح الملف (الوسيط) ببرنامج محرر سداسي عشري (Hexadecimal editor) والذهاب لنهاية الملف تظهر فيه شيفرة نهاية ملف (EOF)، وهي 454F46 بلغة الأرقام السداسي عشرية، والملف الأصلي هنا اسمه "CellPhones.pdf".



رسم 5. برنامج ستيغانوغرافي: شكل جذاب و عمل مخادع!



Hex Editor - [CellPhones.pdf]

File Edit View Tools Window Help

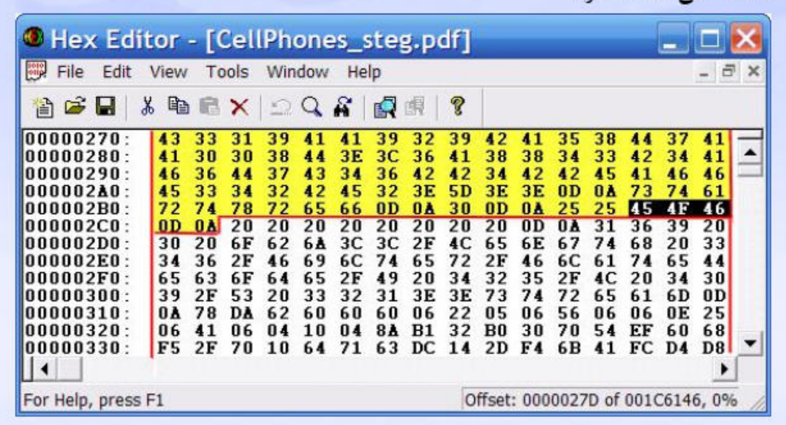
```
00072E60: 30 30 30 30 20 6E 0D 0A 30 30 30 30 34 36 33 36
00072E70: 31 36 20 30 30 30 30 30 20 6E 0D 0A 30 30 30 30
00072E80: 34 36 33 37 34 39 20 30 30 30 30 30 20 6E 0D 0A
00072E90: 30 30 30 30 34 36 33 38 34 32 20 30 30 30 30 30
00072EA0: 20 6E 0D 0A 30 30 30 30 34 36 37 34 37 37 20 30
00072EB0: 30 30 30 30 20 6E 0D 0A 74 72 61 69 6C 65 72 0D
00072EC0: 0A 3C 3C 2F 53 69 7A 65 20 31 34 39 3E 3E 0D 0A
00072ED0: 73 74 61 72 74 78 72 65 66 0D 0A 31 31 36 0D 0A
00072EE0: 25 25 45 4F 46 0D 0A
```

For Help, press F1 | Offset: 00072EE5 of 00072EE7, 99%

رسم **4**. بيانات الملف الوسيط تبين علامة نهاية الملف (EOF).

بعد استخدام برنامج الإخفاء (Steganography 1.8) **فإننا نلاحظ أن البرنامج لم يقم بدمج الملف الثاني داخل الملف الاول بل قام بإلصاقه في نهاية الملف الاول** (Concatenation).

تبين الصورة التالية هذا الإلحاق بحيث تظهر بيانات الملف الأول (الوسيط) باللون الأصفر ويظهر تحتها الملف الذي قام البرنامج بإخفائه! وفي الصورة التي تليها (رسم 7) تم اخفاء نفس الملف وحمايته باستخدام كلمة سر. بمقارنة البيانات في الرسم 6 و الرسم 7 يتبين أن لا علاقة لكلمة السر بتشفير البيانات، فالبيانات في كلتا الصورتين متطابقة بغض النظر عن كلمة السر. وهذا يعني ببساطة أن البرنامج لا يقوم بتشفير البيانات اعتماداً على كلمة السر.



رسم **6**. إخفاء ملف من دون استخدام كلمة سر.



Hex Editor - [CellPhonesstegp.pdf]

File Edit View Tools Window Help

```
00000270: 43 33 31 39 41 41 39 32 39 42 41 35 38 44 37 41
00000280: 41 30 30 38 44 3E 3C 36 41 38 38 34 33 42 34 41
00000290: 46 36 44 37 43 34 36 42 42 34 42 42 45 41 46 46
000002A0: 45 33 34 32 42 45 32 3E 5D 3E 3E 0D  A 73 74 61
000002B0: 72 74 78 72 65 66 0D 0A 30 0D 0A 25 25 45 4F 46
000002C0: 0D 0A 20 20 20 20 20 20 20 20 0D 0A 31 36 39 20
000002D0: 30 20 6F 62 6A 3C 3C 2F 4C 65 6E 67 74 68 20 33
000002E0: 34 36 2F 46 69 6C 74 65 72 2F 46 6C 61 74 65 44
000002F0: 65 63 6F 64 65 2F 49 20 34 32 35 2F 4C 20 34 30
00000300: 39 2F 53 20 33 32 31 3E 3E 73 74 72 65 61 6D 0D
00000310: 0A 78 DA 62 60 60 60 06 22 05 06 56 06 06 0E 25
00000320: 06 41 06 04 10 04 8A B1 32 B0 30 70 54 EF 60 68
00000330: F5 2F 70 10 64 71 63 DC 14 2D F4 6B 41 FC D4 D8
```

For Help, press F1 — Offset: 000002A0 of 000E30A3, 0%

رسم 7. إخفاء ملف و حمايته باستخدام كلمة سر.

4.1 كشف المستور:

قمنا بعدة تجارب لإخفاء ملفات مختلفة داخل أنواع متعددة من الملفات الأصلية، وبعد فتح الملف (الذي يخفي ملفاً آخر) ببرنامج محرر سداسي عشري (Hexadecimal editor) والذهاب لنهاية الملف لاحظنا أن هناك 64 بت تتكرر في جميع الملفات على مقطعين (48491200 و 0084E673) وهي مبينة باللون الازرق في الصور التالية. تعتبر هذه الـ 64 بت نوعاً من العلامة المميزة (أثر) للملفات التي تخفي بداخلها ملفات أخرى، وهذا يعني أنها تكشف وجود ملف مخفي في الملف الأصلي!

4.2 تشفير كلمة السر ام تشفير المعلومات :

قمنا بتجربة إخفاء ملف داخل ملف آخر. في المرة الأولى لم نستخدم أية كلمة سر وفي المرة الثانية قمنا باستخدام كلمة سر، والهدف هنا هو الكشف عما إذا كان البرنامج يقوم بتشفير المعلومات بداخله أم لا. والمفاجأة كانت في انتظارنا.!

لاحظوا أنه في الصورتين (8 و 9) قبل المستطيل الاول باللون الازرق لا يوجد اختلافٌ بين الصورتين، مع أن الصورة الأولى تمثل الملف المخفي من دون تشفير (من دون كلمة سر) أما الصورة الثانية فتمثل الملف المخفي بكلمة سر!. طبعاً لا يوجد اختلاف وهذا معناه أنه لا يوجد أي نوعٍ من التشفير في الإخفاء. وما يقوم به البرنامج هو تخزين بصمة كلمة السر فقط ويعتمد على خوارزمية معدلة لهضم الرسالة (Message Digest) المكونة من 128 بت (16 x 8 بت) أي 16 ثـُمانية. وبعد مقارنة الملف الذي استخدمنا فيه كلمة سر والملف من دون استخدام كلمة سر اكتشفنا مكان تخزين بصمة كلمة السر و هي 128 بت قبل الشيفرة: 0084E673 مباشرة، وما يقوم به البرنامج عند استخدامك لكلمة سر هو فقط حساب البصمة الرقمية لكلمة السر وتخزينها داخل الملف. هذه الطريقة في الحماية لا ترقى حتى لهذه التسمية لأنه لسهولة تخطيها. تم اكتشاف أيضاً أنه من دون كلمة سر توجد البصمة التالية في مكان البصمة الرقمية لكلمة السر، ووجود هذه البصمة الخاصة يعني للبرنامج عدم استخدام حماية في إخفاء الملف. والبصمة الخاصة هي:

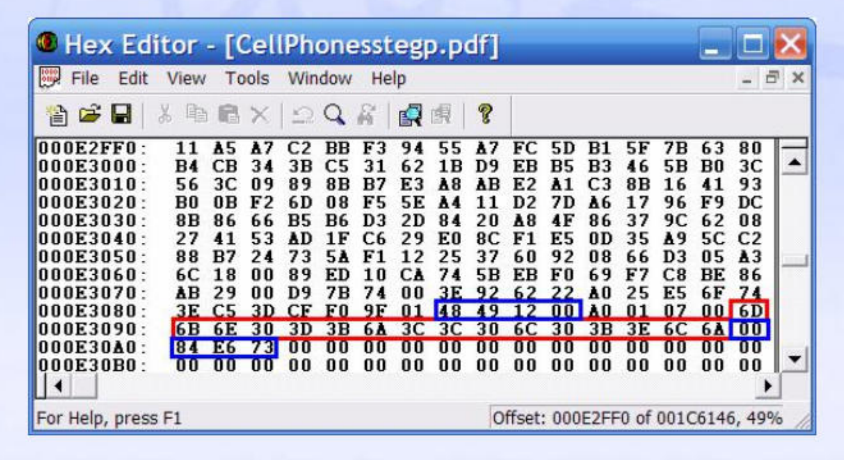
6C 3C 39 6C 30 6B 6C 31 30 6E 38 38 6A 3A 38 3C



ولإلغاء أي كلمة سر تحمي الملف المخفي فإنه عند وجود أية بصمة أخرى يكفي مسحها وتعويضها بهذه البصمة الخاصة باستخدام برنامج محرر سداسي عشري ونكون بذلك ألغينا كلمة السر وبالتالي نقوم باستخراج الملف المخفي بسهولة شديدة من دون معرفة أي نوع من التشفير تم استخدامه في إنتاج البصمة الرقمية لكلمة المرور (كلمة السر)، لأننا نقوم بكل بساطة بإلغاء ما تقول الشركة المصنعة لهذا البرنامج أنه تشفير و هو لا يعدو أن يكون خداعاً في بنية البرنامج!.

```
Hex Editor - [CellPhones_steg.pdf]
File  Edit  View  Tools  Window  Help
000E2FF0:  11 A5 A7 C2 BB F3 94 55 A7 FC 5D B1 5F 7B 63 80
000E3000:  B4 CB 34 3B C5 31 62 1B D9 EB B5 B3 46 5B B0 3C
000E3010:  56 3C 09 89 8B B7 E3 A8 AB E2 A1 C3 8B 16 41 93
000E3020:  B0 0B F2 6D 08 F5 5E A4 11 D2 7D A6 17 96 F9 DC
000E3030:  8B 86 66 B5 B6 D3 2D 84 20 A8 4F 86 37 9C 62 08
000E3040:  27 41 53 AD 1F C6 29 E0 8C F1 E5 0D 35 A9 5C C2
000E3050:  88 B7 24 73 5A F1 12 25 37 60 92 08 66 D3 05 A3
000E3060:  6C 18 00 89 ED 10 CA 74 5B EB F0 69 F7 C8 BE 86
000E3070:  AB 29 00 D9 7B 74 00 3E 92 62 22 A0 25 E5 6F 74
000E3080:  3E C5 3D CF F0 9F 01 48 49 12 00 A0 01 07 00 6C
000E3090:  3C 39 6C 30 6B 6C 31 30 6E 38 38 6A 3A 38 3C 00
000E30A0:  84 E6 73 00 00 00 00 00 00 00 00 00 00 00 00 00
000E30B0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
For Help, press F1          Offset: 000E2FFF of 001C6146, 49%
```

رسم 8. يبين نهاية الملف الوسيط بعد اخفاء ملف آخر بداخله من دون استخدام كلمة سر.



رسم 9. يبين نفس العملية في الرسم السابق و لكن هذه المرة مع استخدام كلمة سر.

4.3 إستخراج المعلومات الخفية بثلاث خطوات:

الخطوات الثلاثة التالية هي لكشف واستخراج أي ملف تم إخفاؤه داخل ملف آخر:

1. البحث عن البصمة 48491200 مع 0084E673 في نهاية الملف. إذا وجدت فهذا يعني أن الملف الظاهر يخفي ملفاً آخر. الخطوة الأولى تنسف فكرة الإخفاء التي يدّعيها البرنامج.
2. نقوم باستبدال بصمة كلمة السر المكونة من 128 بت والموجودة قبل الشيفرة 0084E673 مباشرة ونقوم بوضع مكانها البصمة الخاصة: 6C 3C 39 6C 30 6B 6C 31 30 6E 38 38 6A 3A 38 3C التي تلغي كلمة السر. الخطوة الثانية تنسف من الأساس ادعاء البرنامج حمايته للبيانات باستخدام كلمة سر.
3. نفتح الملف (الوسيط) بالبرنامج نفسه ونستخرج الملف المخفي. الخطوة الآخيرة تبين أن ما كنت تعتقد أنك شفرته وأخفيته بعناية ما هو إلا وهم بحيث يتم استخراجه ببساطة.

و هنا نرد على الشركة المصنعة للبرنامج و التي كتبت الجملة التالية على البرنامج :

Make your secrets invisible in just 3 easy steps!

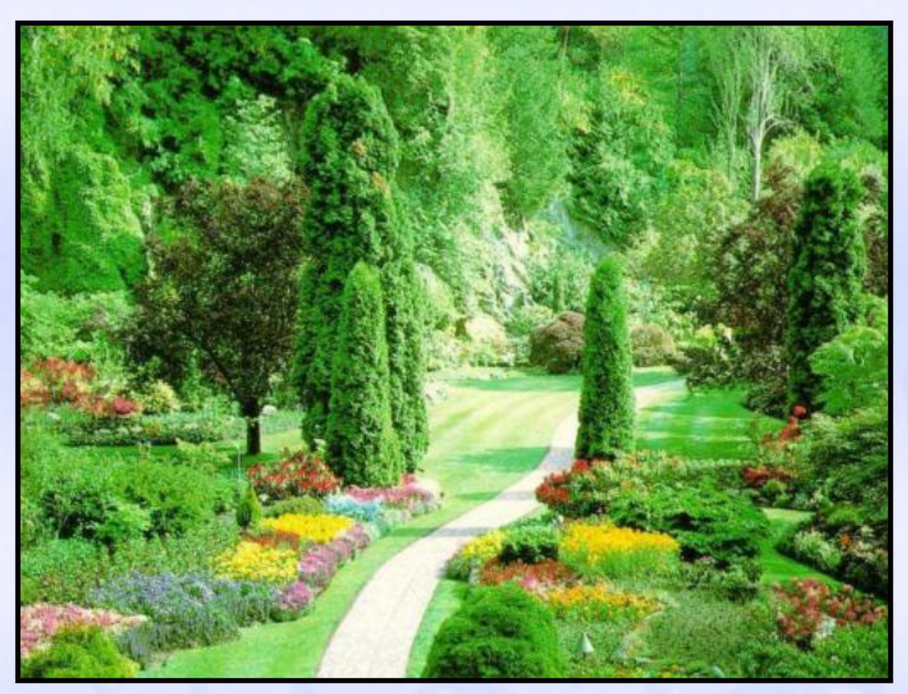
Steganography
Make your secrets invisible in just 3 easy steps !

و الجملة أعلاه تعني: إجعل أسرارك خفية بثلاث خطوت سهلة !. ونقول هنا أنه يتم استخراج أسرارك المخفية أيضا بثلاث خطوات سهلة ! مهما كان نوع التشفير الذي تم استخدامه في هذا البرنامج!.

5. الإخفاء الحقيقي للمعلومات:

في تقنيات الإخفاء الحقيقي فإن الملف الوسيط –وهو إما صورة أو ملف صوتي– يستطيع حمل كمٍّ معين من المعلومات دون أي تغيير في حجم الملف أو في نوعية الصورة أو الصوت. وباستخدام التشفير للبيانات قبل إخفائها نضمن سرِّيَّةً تامَّةً للمعلومات، وهذا يعمل على تعطيل وظيفة تقنيات تحليل الإخفاء اعتماداً على التحليل البصري أو التحليل الإحصائي لعشوائية البيانات المدمجة في طبقات الألوان التي يتم استخدامها في الإخفاء. وبإضافة تقنيات الضغط للبيانات يتم رفع حجم البيانات أو الرسائل المطلوب إخفاؤها. والمثال التالي يبين حجم المعلومات التي يمكن إخفاؤها داخل صورة مثلاً، علماً أن البرنامج الذي يُستخدَمُ هنا غير معروف ولم يتم نشر التقنيات المستخدمة فيه.





المثال 1: الصورة أعلاه بحجم 512×380 بكسل (عنصور) تخفي بداخل ألوانها 200 صفحة من القرآن الكريم، وهذه الصفحات بصيغتها النصية مع التشكيل (أكثر من 240 ألف حرف ،ويشمل ذلك الفراغات والعودة للسطر CR). خوارزمية التشفير المستخدمة 1024 بت ونسبة الضغط 330%، وهذا الإخفاء لا يزيد في حجم الصورة الاصلية ولا بت واحد، فلا يمكن التمييز بين الصورة الأصلية و الصورة التي تخفي بداخلها البيانات.

ويمكن لصورة بحجم 700×800 أن تخفي نص القرآن كاملاً مع التشكيل وترقيم الصفحات وترقيم الآيات. الصور يمكنها أيضاً إخفاء ملفات بجميع أنواعها وليس النصوص فقط، فمثلاً يمكنك أن تخفي برنامج حاسوب أو ملفاً صوتياً أو صورة أو تجميع عدد من الملفات في ملف مضغوط قبل إخفائه داخل الصورة، وهذا كله من دون أية زيادة في الحجم الأصلي للصورة.

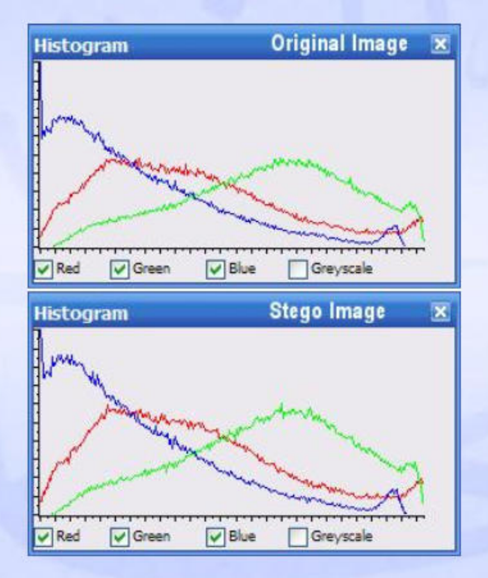


المثال 2: الصورة الصغيرة أعلاه و هي بحجم 50x100 بكسل تخفي 20 بياناً من بيانات الجيش الإسلامي في العراق، أي أكثر من 15 ألف حرف (بما فيها الفراغات)! بنسبة ضغطٍ تصل إلى 1000%. وهذه النسبة العالية من الضغط تنتج بسبب ما يسمى "تكرار بياني" (Data



redundancy)، ويظهر هذا مثلاً في أن جميع بيانات المجاهدين تتكرر فيها بداية البيان ونهايته بينما يختلف محتوى البيان، وهذه البنية تسمح للبرنامج أن يزيد نسبة الضغط. هذه الصور الصغيرة والتي بمقدورها حمل كمٍّ كبيرٍ من الرسائل يمكن نقلها أو إرسالها باستخدام أجهزة الاتصالات الخلوية ضمن رسائل متعددة الوسائط (MMS).

المثال 3: صورة بعرض 500 بكسل و بارتفاع 3 بكسل فقط لا يمكن حتى الانتباه لوجودها، ويمكن لها أن تدخل ضمن تصميم موقعٍ إلكترونيّ في مقدورها إخفاء رسالة بطول يزيد عن عدد أحرف سورة الفاتحة.



رسم **10**. تحليل ترددي للألوان (Histogram) بين صورة أصلية ونفس الصورة بعد إخفاء ما يزيد عن **240** الف حرف! (المثال **1**). التغيير الطفيف لا يؤثر على نقاء الصورة و لا يثير أية شبهة لأن توزيع الألوان يبدو طبيعياً.

6.كيفية اختيار الصور الوسيطة:

اختيار الصورة التي يتم إخفاء المعلومات أو الرسائل بداخلها يخضع لتحليلٍ مسبقٍ لنوعية الصورة. وحتى نضمن قدرةً عاليةً على التخفّي نقوم بتحليل إخفاء (Steganalysis) مسبق للصورة قبل استخدامها، ونعرض هنا ثلاث أمثلة نبين فيها كيفية إختيار الصور المناسبة.

يجب هنا التمييز بين صور الرسوميات (Graphics) والصور الفوتوغرافية (Photos)، فالنوع الأول يحتوي على عدد محدود من الألوان وطبقات الألوان الدنيا لا تخضع كلُّها للتوزيع العشوائي (في المكان) مما يجعل مهمة الإخفاء بداخلها أمراً غير ممكن لسهولة كشفها.



والكشف عن وجود معلومات لا يعني إمكانية معرفة المحتوى فهذا أمرٌ مستحيلٌ لكون خوارزميات التشفير والضغط والإخفاء كلها مجهولة تماماً، ولهذا لا يجب استخدام البرامج الغربية فهي خداعٌ محضٌ وكلها لها نوعٌ من الإمضاء (Signature) يدل على أن الوسيط (صورة) تم تعديله ببرنامج معين.

6.1 تحليل الإخفاء باستخدام التحليل البصَري و الإحصائي.

6.1.1 تحليل بصري - المثال 1:

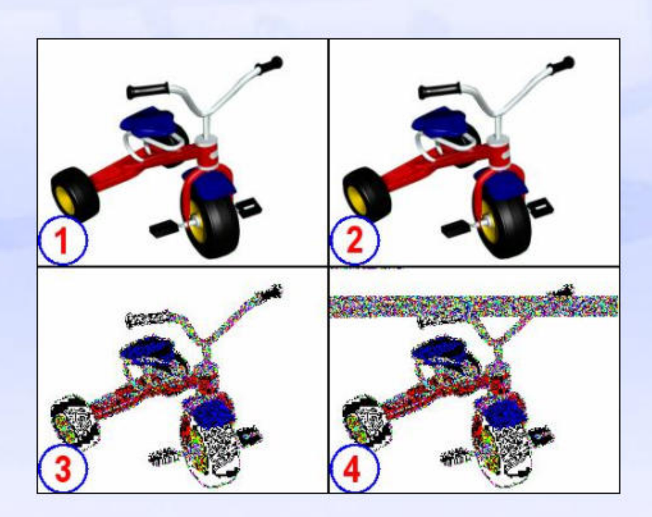
الرسم 11:

الجزء 1: الصورة الأصلية.

الجزء 2: الصورة بعد إخفاء المعلومات.

الجزء 3: التحليل الطبقي للصورة الأصلية.

الجزء 4: التحليل الطبقي للصورة التي تخفي معلومات. ويظهر فيها مستطيل بألوان عشوائية يكشف عن وجود رسالة خفية. بعد الحصول على هذه النتيجة ينتهي دور علم تحليل الإخفاء. والنتيجة إن هذه الصورة غير مناسبة للاستخدام كوسيط للإخفاء.



رسم 11: صورة (رسوميات) تحتوي على عدد محدود من الألوان. يتم كشف الرسائل المخفية بداخلها بسهولة بسبب الخلفية المتناسقة (Homogeneous) من دون القدرة على معرفة المحتوى.



6.1.2 تحليل بصري - المثال 2:

الوسم 12:

الجزء 1: الصورة الأصلية.

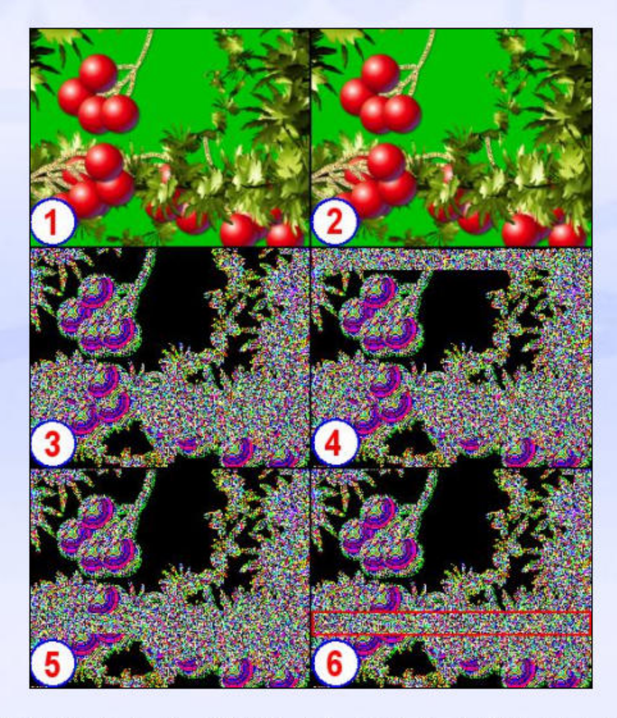
الجزء 2: الصورة التي تخفي الرسالة السرية.

الجزء 3: تحليل طبقي للصورة الأصلية.

الجزء 4: تحليل طبقي للصورة الحاملة للرسالة، يظهر مستطيل من الألوان العشوائية في أعلى الصورة مما يثبت وجود رسالة خفية.

الجزء 5: بعد نقل موقع الرسالة داخل الصورة إلى الأسفل و بالضبط عند المنطقة ذات الألوان العشوائية فيصبح التحليل البصري عاجزاً عن تحديد ما إذا كانت هناك معلومات خفية أم لا.

الجزء 6: نفس الصورة 5 ولكن وضعنا مستطيلاً باللون الأحمر لنبين مكان وجود الرسالة الخفية.



رسم 12: يبين نوعية من الرسوميات يمكن استخدامها لإخفاء الرسائل ولكن يجب اختيار مكان الإخفاء بعناية. وضع الرسالة في المنطقة الخضراء والتي تظهر بالتحليل الطبقي باللون الأسود يجعلها سهلة الكشف.

6.1.3 تحليل بصري - المثال 3،

الرسم 13:

الجزء 1: الصورة الأصلية.

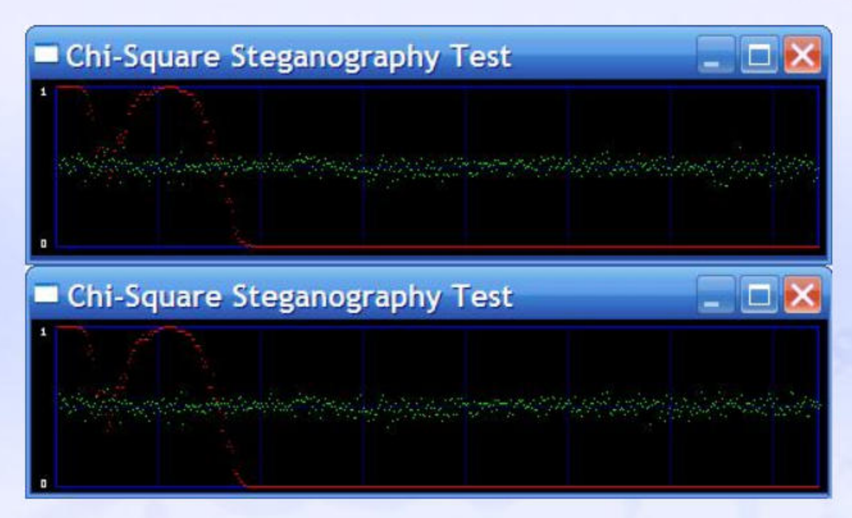
الجزء 2: الصورة بعد أن تم إخفاء رسالة من من 16 ألف حرف وبنسبة ضغط 10 أضعاف، وتشغل الرسالة 9% فقط من حجم الصورة البالغ 190x250.

الجزء 3: التحليل الطبقي للصورة الأصلية.

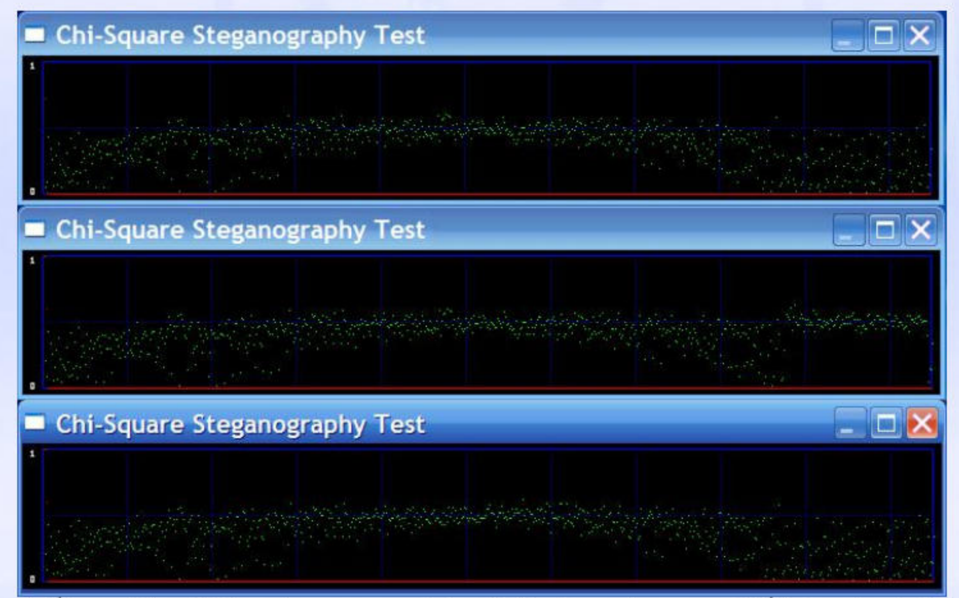
الجزء 4: التحليل الطبقي للصورة التي تخفي الرسالة السرية. طبعاً لا يوجد فرق بين الصورتين باستخدام التحليل الطبقي البصري، وحتى باستخدام تقنيات أخرى في التحليل فلا توجد تقنية يمكنها الجزم 100% بوجود شيءٍ في هذه النوعية من الصور. حتى لو قام برنامج معين بادعاء ألها تحتوي على شيء ما فهذا مجرد احتمال يقبل الصواب والخطأ، ونوعية البرامج التي تحاول الكشف عن الرسائل الخفية اعتماداً على نظرية الاحتمالات تخطئ أيضاً بالنسبة لصور عادية مما يفقد المستخدم لها الثقة بها. ويُعرَفُ الكشف الخاطئ عن وجود معلومات خفية بالكشف الإيجابي الخاطئ (False Positive).



رسم 13: تحليل طبقي يبين ان الصورة أعلاه ذات طيف واسعٍ من الألوان و يتم إخفاء الرسائل بداخلها دون أن تستطيع تقنية التحليل الطبقي البصري اكتشاف رسائل خفية. هذه عينة من نوعية الصور التي يجب استخدامها.



رسم **14**: مثال يبين فشل التحليل الإحصائي (χ^2) في التعرف على الصورة التي تخفي **1.6** كيلو بايت من المعلومات المشفرة. فوق: تحليل الصورة من دون معلومات. تحت: تحليل الصورة مع معلومات مخفية. التحليل يبين أن الصورتين تحتويان على معلوماتٍ مما يفقد التحليل مصداقيته (خاص بالصورة في الرسم **13**).



رسم **15**: التحليل الإحصائي يفشل تماماً في كشف وجود معلومات خفية. الخط الأحمر على المستوى صفر يبين ان الصور الثلاثة التي تم تحليلها إحصائياً لا تحتوي على أي معلومات خفية، بينما في الحقيقة صورتان منهما تحتويان على **1.6** كيلوبايت من المعلومات المشفرة (التحليل خاص بالصورة في الرسم **12**).



7. خلاصة:

المعركة بين علم الإخفاء وتحليل الإخفاء لا تزال محتدمةً وتمثّلُ حجر الزاوية في حرب نقل المعلومات السرية. الوجه الاول لهـذه المعركة يمثل الاتصالات السرية حيث يتم نقل معلوماتٍ و بياناتٍ من دون إشعار أحدٍ أن هناك اتصالاً، بينما يمثل الوجه الآخـر محاولـة الوقوف ضد هذا النوع من الاتصالات. عدة برمجيات تقوم بالوظيفة الأولى وأكثرها له برمجيات مضادة تستطيع الكشف عـن احتمـال وجود رسائل سرية.

وفي حالات كثيرة مثل البرنامج الذي قمنا بتحليله فإن ادعاء إخفاء المعلومات هو محض كذبٍ وخداع، وقد بيَّنَّا كيـف يمكـن استخراج المعلومات التي تم إخفاؤها وحمايتُها بكلمة سر. وهذا ينبهنا أنه لا يجب استخدام أي برنامجٍ من دون أن يكون لدينا تحليلٌ مسبقٌ للبرنامج.

برنامج الإخفاء المتقدم يدمج عدة تقنايات متطورة لانجاز المهمة بكفاءة عالية، حيث يقوم البرنامج بضغط البيانات بنسبٍ عاليـة قبل تشفيرها بخوارزمية 2048 بت وذلك قبل إخفائها. وتقوم بعضُ البرامج بإخفاء رسائل قصيرة داخل ملفات صوتية قصيرة، ومنها مـا يستغلُّ عدداً محدوداً من طبقات الألوان الأساسية محاولاً الإفلاتَ من احتمال كشف أي تغييرٍ عن طريق تحليل الإخفاء الذي يعتمد علـى التوزيع الإحصائي للألوان. وتقوم برامج أخرى بإخفاء البيانات أو الرسائل عن طريق استغلال أحدث التقنيات في عالم هندسة الاتصالات و هي ما يسمى الطيف العريض (Spread Spectrum) لتفلت من جميع الإجراءات المضادة لتحليل الإخفاء. كما بيَّنَّا كيفية اختيار النوعية المناسبة من الصور الفوتوغرافية أو الصور الطبيعية التي يعجز التحليل البصري بالإضافة للتحليل الإحصائي عن الكشف عن احتوائها على رسائل خفية، مما يجعل علم الإخفاء يستحق بجدارة هذا الاسم وينفرد بنقل المعلومات السرية دون أن تراها الأبصار.

قال الله تبارك و تعالى في سورة الحاقة: ((فلا أقسم بما تبصرون و ما لا تبصرون)).

مصطلحات مهمة

Steganography (Steganos graphy)	علم الإخفاء
Steganalysis	تحليل الإخفاء
Multi-media	وسائط متعددة
Digital	رقمي
Morse Code	شيفرة مورس
Digital Communication	إتصالات رقمية
Digital Signal and Image Processing	معالجة الإشارة و الصور الرقمية
Watermarking	العلامة المائية



LSB (Least Significant Bit)	البت ذي الدلالة الصغرى
MSB (Most Significant Bit)	البت ذي الدلالة الكبرى
Pixel (Picture element)	عنصر صورة (عنصور)
Grayscale	السلم الرمادي
Message Digest version 5 (MD5)	هضم الرسالة: تقنية خاصة بتشفير كلمة السر
Byte	ثمانية (بضم الثاء و تشديد الياء)
Bit	بت
Hexadecimal	سداسي عشري
Editor	محرر
Concatenation	الالصاق او الالحاق
Digital Fingerprint	البصمة الرقمية
Data Redundancy	تكرار بياني
Histogram (Frequency distribution of RGB)	هيستوغرام (رسم بياني لتوزيع الالوان الترددي)
One Way Encryption	تشفير أحادي الإتجاه
Discrete Cosine Transform (Coefficients)	التحويل الجيبي المتقطع (معاملات)
Enhanced LSB Layers Analysis	التحليل الطبقي
Visual Analysis	التحليل البصري
Statistical Analysis	التحليل الإحصائي



كيف تنشئ موقعاً جهادياً من الألف إلى الياء (الجزء الأول)

بقلم: أبو دجانة المكي

الحمد لله رب العالمين، والصلاة والسلام على خير الأنبياء والمرسلين سيدنا محمد، وعلى آله وأصحابه الطيبين الطاهرين، ومن تبعهم بإحسانٍ إلى يوم الدين.

أما بعد..

هنا سنبدأ بحول الله وقوته سلسلةً تشرح للإخوة أنصار الجهاد كيفية إنشاء مواقع جهادية لنشر فكر المجاهدين وعملياتهم؛ ليظهر للعالم حقيقة المجاهدين وعملياتهم وأهدافهم.

السلسلة ستكون في عدة حلقات. وفي هذه الحلقة سنشرح وبشكلٍ مبسَّطٍ جداً أُسُسَ البحث عن أفضل شركة استضافة، ثم سنشرح الأمور المتعلقة بالدومينات من أنواعها وحجزها وغير ذلك .

General account information:

Hosting package	Staff
Shared Ip Address	[illegible]
Subdomains	7 / unlimited
Parked Domains	1 / 999
Addon Domains	0 / 999
MySQL Databases	2 / unlimited
Disk usage	1324.30 Megabytes
SQL Disk usage	0.02 Megabytes
Disk space available	Unlimited Megabytes
Bandwidth usage (current month)	97.25 Megabytes
Email Accounts	5 / unlimited
Email Forwarders	2
Autoresponders	0
Mailing Lists	0 / unlimited
Email filters	0
Ftp Accounts	10 / unlimited

General server information:

Operating system	Linux
Service Status	Click to View
Kernel version	2.6.10
Machine Type	i686
Apache version	1.3.33 (Unix)
PERL version	5.8.1
Path to PERL	/usr/bin/perl
Path to sendmail	/usr/sbin/sendmail
Installed Perl Modules	Click to View
PHP version	4.3.10
MySQL version	4.0.22-standard-log

1. مكونات الموقع (ما هو الموقع):

الموقع يتكون من قسمين:

1) مساحة الموقع : وهي المساحة التي تضع عليها ملفاتك وصفحاتك، وهي الموقع الخاص بك فعلاً. ويتم حجزها من شركات استضافة hosting.

2) اسم للموقع : وهو الاسم الذي تتعامل به مع الزائر، وهو بمثابة عنوان الاستضافة. فالإنترنت كالمدينة الكبيرة وبحجزك للمساحة تكون متواجداً على الشبكة لكنك تحتاج أيضاً إلى عنوانٍ لكي يصل إليك زوارك domain.



2. خطط حجز المواقع:

هناك شركات تعطي مساحات مجانية ولكن هذه الشركات لا تكون أمينةً عليك وعلى ملفاتك، وتختفي كل بضعة أيام في ظروف غامضة ولها أغراض مثل إضافة إعلانات تجارية في صفحاتك وغير ملتزمة بشيء. لن نتكلم عن هذه الشركات بل عن الشركات المدفوعة.

2.1 نصائح مهمة:

1) كن مع الأجنبي (مع أسفنا لهذا): هناك الكثير من شركات الاستضافة من جنسيات متنوعة، فهناك العرب وهناك غيرهم. هناك مشكلات لصيقة بشركات الاستضافة العربية التي يديرها شخص واحد غير ملتزمٍ بك تماماً، والخطط المرتفعة الثمن، والمزايا المنخفضة، والتعطل، وأحياناً كثيرة التعامل السيئ ومساومتك على ملفاتك أو قواعد بياناتك.

2) اسأل عن السمعة والعملاء: لا تحجز موقعك لدى شركة وليدة اليوم أو حتى هذا العام، ولا تحجز لدى شركة تعذب عملاءها – يمكنك معرفة العملاء بطرق مختلفة كذلك يمكنك سؤال الدعم الفني لدى الشركة نفسها– بل احجز لدى شركات موثوقة، وانظر سرعة التحميل منها وسرعة الرد من سيرفراتها ping host.com -t .

3) تأكد من خدمات الدعم الفني: الدعم الفني هو شيءٌ مهمٌ قد تحتاجه، فقد يتوقف الموقع وقد تحدث لديك مشكلات، وفي هذه الحالة فإن الدعم الفني هو من يمد لك يد العون ويجيب على استشاراتك وطلباتك. هل هو يقظ؟ هل هو متعاون بالطريقة التي تحتاجها؟ أنت تعرف موقعك وتعرف ما سيحتاجه ..

4) ماذا سيحتاج موقعك: أحياناً يحتاج بعض الإخوة إلى فتح موقعٍ لغرضٍ بعينه أو يحتاج أشياء بعينها. فمثلاً تريد فتح موقع وتريد وضع سكريبت رفع يعتمد على الدالة copy، هل سألت الدعم الفني قبل الحجز عن الدالة كوبي فبعضهم يغلقها!. تريد إرسال بريد من قائمة بريدية تعتمد على mail، بعضهم يغلقها فهل تأكدت أنها مسموحة لموقعك؟ تحتاج إلى سيف مود مغلق مثلاً وهكذا... هناك أشياء أنت تعرف أنك ستحتاجها وقد تكون مغلقة.

5) نوع السيرفر وعدد المواقع عليه: قد تحتاج لمعرفة نوع السيرفر وعدد المواقع عليه، فنوع السيرفر وسرعته تؤثر على سرعتك، والسيرفر جهاز كمبيوتر مثل أي جهاز يمكنك أن تسأل عن مواصفاته وعن عدد المواقع عليه والتي تؤثر على سرعتك.

6) فترة الوجود على الشبكة: السيرفر قد يتوقف للحظات ثم يعود وهناك وسائل مراقبة لذلك، فيتم حساب وقت وجود السيرفر واتصال المواقع بالشبكة وقياس ذلك بالنسبة المئوية مثل 99.8% وهي تسمى Up Time.



2.2 المزايا والخطط المختلفة للاستضافة:

استضافتك حيث تضع ملفاتك وصفحاتك وحيث تعمل برمجياتك –مثل المنتديات وغيرها– تحتاج مساحةً، ونقل بيانات، ووسائل عمل برمجيات وغيرها... ما معاني هذه الكلمات وكيف تضع الشركة خطط استضافتها ؟

1) المساحة : تصدر الشركات مساحة الاستضافة ويكون القياس بالجيجابايت GB أو بالميجابايت MB وتسمى (Space, Storage). المساحة تكون هامةً لك حيث تضع ملفاتك، فهل ستضع ملفات صفحات بسيطة فلن تحتاج مساحة؟ أم صوتيات ومرئيات؟ وهل ستضع الملفات على الموقع أم في مواقع رفع مختلفة؟ .

2) تبادل البيانات: يكون البيان التالي غالباً هو سعة تبادل البيانات وهي ما يتم تحميله من موقعك، فكل ما يتم تحميله من موقعك يتم حسابُه وغيرُ مسموحٍ بالتحميل من موقعك إلا بقدرٍ محدودٍ غالباً، وهي تحسب شهرياً غالباً، وقد توضع شروط يومية.
لنفترض أن لديك ملف **100** ميجا وسعة تبادل البيانات **10** جيجا، إذن إذا تم تحميل هذا الملف من موقعك مائة مرة بعدها سيتم تعطيل موقعك حتى نهاية الشهر.
الصفحات لا تأخذ سعة تبادل بيانات كبيرة لكن في حالة كبر حجم الزوار تكون مؤثرةً بالطبع. ويتم حساب سعة البيانات بالجيجابايت GB وتسمى: (Transfer , Bandwidth).

3) خطط ضخمة غير حقيقية: أحيانا تجد عروض ضخمة جدا مثلا مساحة **300** جيجا وبسعر قليل جدا هذا يسمىoversell وهو أن الشركة تقوم ببيع مساحات لا تملكها في حقيقة الأمر لعلمها أنه لا أحد سيستخدمها فـ**90%** لا يستخدمون **10%** من حصصهم . موقعك لن يحتاج كل هذه المساحة وإن احتاجها فهذا يعني انه يستخدم الكثير من موارد الجهاز CPU-RAM وقد يتم إيقاف موقعك .هنا تأتي أهمية سؤال عملاء الشركة وسؤال الخبراء عما يحتاجه موقعك حقيقة وهل يستغل الكثير من موارد النظام هذا قد يدفعك للبحث عن سيرفر خاص او سيرفر شبيه بالخاص VPS.

4) قواعد البيانات: تحتاج إلى قواعد بيانات في الكثير من البرمجيات في موقعك. قد تحتاج أكثرَ من قاعدة، ويمكنك أن تضع أكثر من برنامج على نفس القاعدة لكن هذا غير مستحسن.
وهناك أكثر من نوع من القواعد، وأنت قد تحتاج نوعاً بعينه فأسأل عنه. لكنَّ العامَّ أنَّ قواعدَ MySQL هي العامة.
تجد هنا عدد قواعد البيانات، وكذلك هناك مواقع تضع حدوداً لحجم القواعد، فيضع حدًّاً أن قاعدة البيانات يكون حجمها أقل من **50** ميجا مثلاً، علما أن قواعد البيانات تأخذ الحجم من المساحة، وقد لا تكون هناك حدود فيكون لا نهائياً .

5) البريد الإلكتروني: تحتاج لبريد إلكتروني لموقع ليكون أساس التراسل معك فيكون بمثابة البريد الرسمي، وقد تكون هناك حدودٌ على عدده أو مساحته وقد لا تكون هناك حدود فيكون لا نهائياً.

6) دعم PHP: وهو دعم للغة البرمجة PHP، وهي برمجيَّةٌ هامَّةٌ جداً يعمل على أساسها أغلب برامج الويب.
وهي تعتبر افتراضياً موجودةً في كلِّ الاستضافات لأهمِّيتِها، وقد لا يتم كتابتها باعتبار وجودها شيئاً طبيعياً، لكن وجود قواعد البيانات يكون بمثابة الدليل على وجودها.



كما يجب التأكيد على إصدار PHP، فالكثير من البرمجيات تعتمد على إصدار PHP4. فهل السيرفر يدعم PHP4 أم PHP5؟ وما الذي تحتاجه أنت فقد تحتاج PHP5 وليس PHP4.

7) دعم Perl: وهي دعم برمجية Perl. تستخدم غالبا في التطبيقات المتقدمة و قد لا تكون بحاجة اليها في هذه المرحلة.

8) دعم CGI: وهي لغةٌ برمجيةٌ مهمة، وقد تحتاجها وتعمل عليها برمجيات متنوعة، وهي منتشرة و يفضل الحصول على هذه الخاصية.

9) لوحة التحكم: هناك أنواعٌ مختلفة للوحة التحكم. لوحة التحكم تسهل عليك التحكم في موقعك وإدارته، من عمل قواعد بيانات، أو إدارة بريد، أو إدارة الملفات وغيرها... وهناك لوحات تحكم شهيرة ومفيدة مثل CPanel.

10) SSL: وهي للروابط المشفرة https. ويكون لها سعرٌ ورخصةٌ وأيبي خاص بك. قد تكون مجانيةً وقد تكون بسعر معين.

11) رسوم الإعداد : قد تجد مبلغ رسوم إعداد تُدفع أول مرة فقط، وتكون غالباً إذا حجزت لفترة قصيرة، وهي لضمان جِدِّيَتك، والغالب أنها غير موجودة.

12)) الدومينات المركونة: وهي لإضافة أكثر من دومين لموقعك. فإذا كان لديك أكثر من دومين لنفس الموقع فأنت تحتاج هذا الخيار وتسمى (Parked Domains).

13) الدومينات المضافة: وتحتاجها لوضع أكثر من موقعٍ على استضافتك، فيكون لديك استضافة واحدة تحمل أكثر من موقعٍ مختلف تماماً بالنسبة للزائر، ويكون ذلك بعمل مجلد وربطه بالدومين الأخر. وتكون محددةً بعدد أو لا نهائية وتسمى (Addon Domains).

14) البرامج الإضافية : تكون هناك برامج إضافية يتم إضافتها للوحة تحكُمِك، وتكون مفيدةً لك مثل (Fantastico).

15) إضافات مجانية: تكون هناك أحياناً إضافاتٌ مجانية، مثل دومين مجاني أو SSL أو IP خاص أو حتى فترة مجانية إضافية.

16) نظام تشغيل السيرفر: نظام تشغيل السيرفر يؤثر عليك، فهناك سيرفرات اللينكس التي تتميز PHP كلغة برمجية وMySQL كقواعد بيانات، وسيرفرات الوندوز التي تتميز بـ ASP كلغة برمجية وقواعد بيانات Access و MSSQL.
وهناك فرق السعر فسيرفرات الوندوز أغلى، ليس لأنها أفضل لكن لأن الوندوز نفسها تحتاج رخصةً تتكلف الشركات لشرائها، وعامَّةً سيرفراتُ اللينكس هي الأشهر وهي الأفضل.

17) ضمان استعادة المال : يكون هناك خيار لاستعادة المال بعد فترة معينة من التجربة، ويكون في الشركات الكبيرة، ويكون بعد فترة غالباً 30 يوماً أو كما تحدد شركة الاستضافة وتسمى (money back guarantee).

3. الدومينات (Domains):

الدومين هام جداً لك، فهو ما يعلق بذهن الزائر، وهو الذي يعبر عنك وعن موقعك، وهو الذي يبقى معك أكثر من الاستضافة. فقد تترك الاستضافة في أية لحظة ولكن لن تترك الدومين، وعند تغيير الاستضافة لن تخسر زوّارك ولن تخسر سمعتك بعكس تغيير الدومين. ولّما كان ذلك كان عليك أن تحرص في اختيار الدومين..



3.1 نصائح مهمة:

1) ابحث عن الأكبر: تكون هناك شركات صغيرة تأخذ توكيلاً أو رخصةَ موزع لشركاتٍ أكبر منها. لا تشتري من هذه ولكن كن مع الأصل، كن مع الأكبر.

2) لا تضع البيض في سلة واحدة: لا تحجز الدومين من شركة الإستضافة إن أمكن، ولا تترك شركة الاستضافة تحجز لك من أي مكان ولا تعطيك لوحة تحكم للدومين، إذ لا بد من أن يكون لديك لوحة تحكم للدومين.
فبعض المستضيفين الخبثاء لا يعطون العملاء لوحة تحكم للدومين ثم يساومونهم عليه بسعرٍ مرتفع، وأيضاً إن تم إيقافُك من قبل الشركة المضيفة تتحول لغيرها بسهولة بعكس الدومين.

3) اسأل عن السمعة والعملاء: لا تحجز موقعك لدى شركةٍ وليدةَ اليوم أو حتى هذا العام، ولا تحجز لدى شركة تعذب عملاءها. هناك شركات معروفة وعالمية سمعتها تسبقها.

4) المزايا : قد تحتاج مزايا بعينها من الدومين، فأنت صاحب سيرفر وتريد نيم سيرفر فهل الشركة تتيح لك هذا بسهولة؟ أو مثلاً تريد إخفاء معلوماتك فهل تتيح هذا بسعر مناسب؟ وهكذا...

5) لا تقلق من عدم وجوده: عند حجز الدومين قد تجد أن الدومين غير موجود على الشبكة بعد ربطه بالاستضافة، فلا تتعجب فقد تمر دقائق أو ساعات حتى تربط شركات الاتصالات الدومين باستضافتك، وهذا متوقف على مزود خدمة الإنترنت لديك فإذا دخلت ببروكسي قد تجد الموقع ولكن بمزود الخدمة العربي البطيء قد تنتظر ساعات أو قد يصل ذلك ليوم فلا تقلق.

6) عبِّر بالدومين: اختر اسماً معبِّراً للزائر، فإن كان اسم الموقع "الإخلاص" فليكن الدومين هو كلمة "الإخلاص" بحروف لاتينية، وضع لاحقةً مناسبة، علماً أن الزوار يبحثون عن اللاحقة com. أولاً باعتبارها الأشهر.

7) دقق في الاسم: تأكد من سهولة حفظ الموقع بصورة سليمة وهجائه السليم إن كان لاتينياً، وبساطته إن كان عربياً قمتَ بكتابته بحروف لاتينية. قم بتجربته مع أكثر من أخ.

8) أغلق الدومين: في لوحة تحكم الدومين تجد خيار إغلاق الدومين، وهذا الخيار لمنع نقل الدومين من شركة لأخرى والذي قد تحتاجه أنت أو يحتاجه غيرك لسرقة دومينك.

3.2 المزايا والمصطلحات المختلفة للدومينات:

1) أسماء مختلفة: هناك أسماء مختلفة للدومينات، كلٌّ منها يعني أمراً ما، قد يعني اسماً لدولة ما أو نوعيةَ الموقع واهتمامه. هذه الأسماء تختلف بينها في السعر أيضاً، فهناك أنواع أرخص مثل info. وأنواع اغلي مثل tv. بالطبع الأشهر والأسهل com. بسبب الشهرة والسهولة في ضغط Ctrl+Enter.

2) عروض خاصة: أثناء حجزك للموقع تجد عروضاً خاصة بدومينات أو باستضافة أو أشياء تكون مفيدة لك، قد تجد الإشارة موجودة عليها فلتُزِلْها إن لم تحتجها.



3) خصوصية معلومات التسجيل: يكون هناك لكل دومين مجموعة من المعلومات والتي تعرض للعامة ولكل باحث عنها، منها اسم وعنوان وبريد وأشياء من هذه أنت الذي تضعها، وهي مختلفة عن بيانات الدفع، فتستطيع كتابة معلومات مغلوطة بالطبع. وأيضاً يمكنك شراء خدمة خصوصية معلومات التسجيل (Private Registration) فلا يتم عرض معلومات عنك، وهذه الخدمة قد تشتريها وقد تكون مجانيةً في بعض الحالات.

4) سعر التجديد: أحيانا تكون هناك خدعة وهي جعل سعر الدومين رخيصاً ولكن سعر التجديد بعد عام يكون أغلى من المعتاد، فالسعر الأول يكون لكسب زبائنَ للشركة والثاني لتعويض الأول، فلا تغتر بالأول فقط ولكن انظر في أسعار التجديد.

5) شهادة SSL: وهي شهادة لضمان SSL، وتكون بسعر إضافي ومنها 128 أو 256 bit.

3.3 لربط الدومين مع الاستضافة:

لربط الدومين مع الاستضافة يتوجب عليك العمل من ناحيتين: العمل من ناحية الدومين لإخباره بالسيرفر المحتوي على موقعك، والعمل في استضافتك لإخبارها بدومينك.

في لوحة تحكم الدومين تجد خيار Name Server أو NS، في هذا الاختيار تستطيع تعديل اسم موقعك والذي هو غالباً يكون من عنوانين أو أكثر بهذه الصورة NS1.host.com // NS2.host.com

المعنى	الدومين	المعنى	الدومين
تجاري	.com	الإمارات	.ae
شبكات	.net	سوريا	.sy
المنظمات	.org	أفغانستان	.af
معلومات(وهو من أرخص النطاقات)	.info	بريطانيا	.uk
منظمة أعمال	.biz	إسرائيل	.il
موقع (Web Site)	.ws	السعودية	.sa
تليفزيون	.tv	العراق	.iq
شخصي	.name	الأردن	.jo
تعليمي	.edu	مصر	.eg
حكومي	.gov	إيران	.ir

4. خلاصة:

في هذه المقالة تم شرح الخطوات الأساسية الأولى عندما نقرر إنشاء موقع جهادي على الانترنت. فبعد اختيار شركة الاستضافة وخطة الاستضافة والدومين يكون الموقع قد أنشئ، وفي الحلقات القادمة سنشرح كيف تتم إدارة الموقع و تنزيل المواد عليه حتى ينتهي بنا المطاف بموقع جهادي متكامل إن شاء الله.



الأسلحة الذكية: صواريخ أرض ـ جو قصيرة المدى (الجزء الأول)

بقلم: أبو الحارث الدليمي



صواريخ أرض- جو أو الصواريخ المضادة للطيران تنقسم إلى ثلاثة أنواع: قصير المدى، متوسط المدى وبعيد المدى. القسم الثاني والثالث يطلق من منصة إطلاق صواريخ ضخمة ويصل مداه إلى **200** كلم أو يزيد، أما النوع الأول فهو محمول على الكتف يمكن لشخص واحد إطلاقه ليلاً أو نهاراً، ويصل مداه إلى **10** كلم. ومن أشهر هذه الصواريخ الصاروخ ستنجر (رسم **1**) والصاروخ إيغلا الروسي، وهما من أحدث الصواريخ المحمولة على الكتف. هذا النوع من السلاح فعال للغاية لإسقاط الطائرات بجميع أنواعها.

الصاروخ هو نوع ذكي مجهز برأس يحتوي على كميرا للتصوير الحراري والتي تقوم بالتقاط الأشعة تحت الحمراء المنبعثة من محرك الطائرة واللحاق بها. نظام الباحث الحراري هو نظام تعقب ذكي يقوم بتتبع مصدر حرارة المحرك والتحليق بسرعة عالية تصل إلى ضعف سرعة الصوت ليتمكن من إسقاط أي طائرة تحلق في ارتفاع يقل عن **3500** متر ولا يزيد بعدها عن **4** كلم.

سوف نشرح لاحقاً إن شاء الله كيفية عمل هذا النوع من الصواريخ وكيفية استخدامه وفعاليته، ونتعرف على الدور الذي يلعبه ضد الاحتلال الأمريكي في العراق، في أفغانستان وضد الاحتلال الروسي في الشيشان.



رسم **1**. صاروخ ستينجر (**FIM92**) أرض – جو من إنتاج شركة رايثيون. الصاروخ تطور إنتاجه بعدة نسخ منها النسخ **A,B,C,D,E,F** بالإضافة لنسخة جو- جو **ATAS** المستخدمة في سلاح الجو.



1. تعريف بالصواريخ الذكية أرض- جو قصيرة المدى:

صاروخ أرض – جو قصير المدى تم تصميمه ليمنح القوات البرية طريقة فعالة للتعامل مع الطائرات والمروحيات التي تحلق على ارتفاع منخفض. من منظور المجاهد على الأرض فإن الطائرات المعادية التي تحلق على ارتفاعٍ منخفض تشكل خطراً حقيقياً لأنها تكون إما في مهمة قصف، أو مراقبة، أو إنزال جنود أو استخراجهم، أو إعادة تموين لقوات العدو (رسم 3–4). وإسقاط هذه الطائرات هي أسهل طريقة للقضاء على هذا الخطر.

خير مثال نذكره هو عمليات إسقاط 10 مروحيات في شهر واحد شملت جميع أنواع المروحيات مثل الأباتشي ، بلاك هوك، الشينوك، وحتى إسقاط طائرة من نوع إف–16 في منطقة الكرمة غرب بغداد، والعملية الأخيرة نفذها مجاهدو دولة العراق الإسلامية بالتعاون مع جيش المجاهدين وكان ذلك يوم الإثنين الموافق لـ 27/ 11/ 2006.



رسم 2. مجاهدو دولة العراق الإسلامية يطلقون صاروخ أرض– جو على مروحية شينوك في منطقة الكرمة. ثواني فقط فصلت إطلاق الصاروخ على تحويل المروحية بمن فيها من جنود إلى كتلة من لهب. الصورة الوسطى تبين الصاروخ الموجه قبل إصابته للهدف. العملية بتاريخ 7/ 2/ 2007 نشرتها مؤسسة الفرقان للإنتاج الإعلامي

تستخدم الصواريخ تستخدم مجساتٍ حرارية أحادية اللون للأشعة تحت الحمراء تعمل في المجال 3–5 ميكرون لالتقاط الإشعاع المنبعث من محرك الطائرة والناتج عن ثاني أكسيد الكربون (CO_2)، وهذا الإشعاع مُرَكَّزٌ عند طول الموجة 4.2 ميكرون، كما أن هناك مجسات أحدث تشبه إلى حد كبير كاميرات حرارية تعمل في المجال 8–13 ميكرون مما يعطيها مقاومة عالية ضد الإجراءات المضادة، كما أن هذا المجال الترددي يقل امتصاصه من الجو وهذه المجسات تعرف بثنائية اللون. وأحدث مجسات مستخدمة هي InSb و HgCdTe.

من المميزات التي تجعل هذا النوع من الصواريخ سلاحاً فعالاً لاستخدام المجاهدين هي أن هذا السلاح خفيفٌ ونقال، الصاروخ مع القاذفة يزنان ما بين 15 و 18 كغ، علماً أن القاذفة يعاد استخدامها والصاروخ وحده يزن ما بين 10 و 11 كغ. شخصٌ واحدٌ يمكنه حمل القاذفة وإطلاق الصاروخ ليلاً أو نهاراً. هذا النوع من الصواريخ تطلق عليه عبارة "أطلق وانسحب"، حيث أنه بعد إطلاق الصاروخ مباشرةً يمكن الانسحاب من الموقع، ويقوم الصاروخ بتعقُّب الهدف تلقائياً عن طريق الحاسوب المدمج بداخله والذي يعتمد على نظام



معالجة صور رقمية حرارية، ونتائج التحليل يتم توجيهها لنظام التحكم الآلي الذي يوجه الصاروخ نحو الهدف، وذلك بتغيير اتجاه أجنحة القيادة الأمامية، ويعرف هذا النمط من التحكم في هندسة التحكم بنظام التحكم المرتجع (Feedback Control System).

هذا السلاح ذو ميزات جذابة و لهذا فان الكثير من الجيوش عملت ليس على اقتنائه فحسب بل وتصنيعه ليكون حجر زاوية في منظومتها الدفاعية.



رسم **3**. الطائرات المروحية هدفٌ سهل لصواريخ أرض– جو ذات التتبع الحراري. هنا تظهر طائرة بلاك هوك (الصقر الأسود) الخاصة بالإنزال الجوي والتي تم إسقاط عددٍ منها من ضمن **10** مروحيات في خلال شهر واحد..

الباحث الذي يعمل بالأشعة تحت الحمراء قادرٌ على ملاحقة الحرارة التي ينتجها محرك الطائرة، ويسمى الباحث "سلبي" لأنه على خلاف الصواريخ الموجهة بالرادار فإنه لا يحتاج إلى موجاتٍ يبثها رادار من منصة أرضية ليلاحق هدفه بل يقوم بمتابعة هدفه تلقائياً من دون مساندة أرضية. الصاروخ يعمل بالوقود الصلب ذي الاحتراق العالي، وحمايةً للشخص الذي يحمل القاذفة على كتفه من نار المحرك فإنه يتم إطلاق الصاروخ على مرحلتين: المرحلة الأولى يتم فيها قذف الصاروخ خارج أنبوب القذف بحيث يبتعد الصاروخ عن الشخص بمسافةٍ كافية، ثم يتم تشغيل محرك الصاروخ تلقائياً لينطلق الصاروخ بسرعةٍ تصل إلى ضعف سرعة الصوت أو تزيد.



رسم **4**. مروحية بلاك هوك من الداخل. الدائرة الحمراء تظهر شاشة الرؤية الليلية بينما تظهر الدائرة الزرقاء شاشة نظام تحديد الموقع بالأقمار الاصطناعية مع نظام الخرائط الرقمية (جي بي آس– جي آي أس).



2. صاروخ أرض - جو: كيفية الاستخدام؟

لإطلاق الصاروخ يقوم المجاهد بمتابعة الهدف عن طريق منظار الصاروخ، ويقوم نظام الإطلاق والمبنيٍّ أساساً على الباحث الحراري بإصدار إشارة خاصة تبين أن الهدف (الطائرة) موجودٌ في مجال تغطية الصاروخ، ويعرف هذا بالإقفال. عندها يضغط المجاهد على زناد الإطلاق وحينها يقوم محرك الإطلاق بقذف الصاروخ خارج أنبوب القاذفة المحمولة على الكتف، وهكذا يكون الصاروخ قد ابتعد مسافةً كافية عن المجاهد بعدها يقوم الصاروخ تلقائياً بتشغيل محرك الصاروخ الأساسي الذي يعمل بالوقود الصلب، فينطلق الصاروخ بسرعة عالية تصل في بعض الأنواع إلى **2448** كلم/ساعة، وهذا يعادل ضعف سرعة الصوت أو ما يعرف بـ ماخ **2** (رسم **5-6**).



رسم **5**. يمين: المكونات الأساسية لصاروخ أرض – جو ستنجر يعمل بالأشعة تحت الحمراء: **1**– محرك إطلاق، **2**– محرك الوقود الصلب للصاروخ، **3**– الرأس الحربي، **4**– نظام القيادة الآلي، **5**– الباحث الحراري: كميرا رقمية للتصوير الحراري.

يسار: المكونات الأساسية لقاذفة صاروخ محمولة على الكتف: **1**– أنبوب الإطلاق، **2**– زناد الإطلاق، **3**– منظار الإطلاق، **4**– هوائي نظام اتصالات للتعرف على الطائرات الصديقة والمعادية (اختياري).



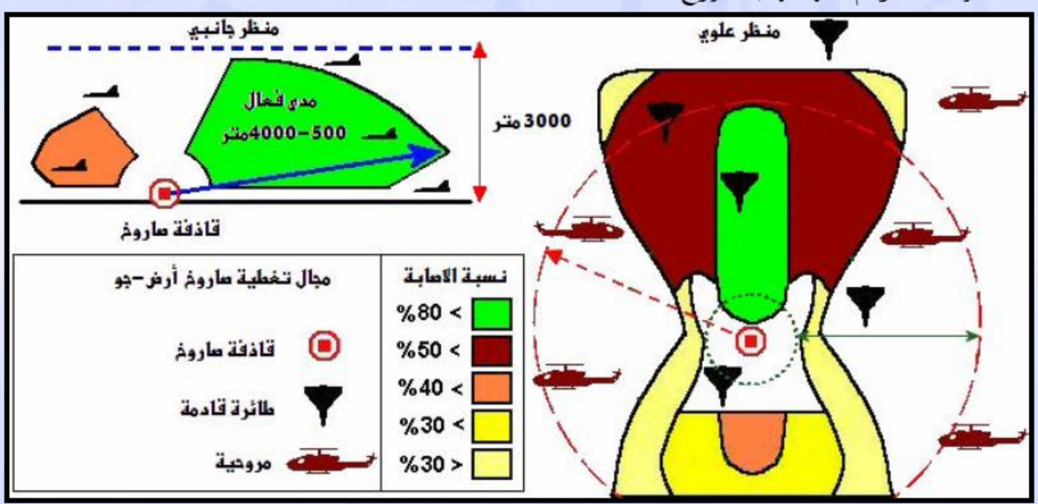
رسم **6**. مجاهدين من حركة طالبان في إمارة أفغانستان الإسلامية يترصدون الطائرات المعادية بصواريخ أرض– جو (يمين).

أحد المجاهدين يطلق صاروخاً على مروحية أمريكية في بلاد الرافدين (يسار)



باستطاعة الصاروخ التحليق لعلوٍّ يصل إلى 3000 متر وملاحقة أي هدف إلى مدى يصل حتى 8 كلم. عموماً هذا يعني أنه باستطاعته وبنسبة عالية تدمير أي طائرة تظهر في الجو بشرط أن تكون واضحة بشكلها الخارجي ولا تظهر كنقطة في الجو. النسخ الحديثة من هذا النوع من الصواريخ يمكنها أيضاً التغلب على الإجراءات المضادة التي تستخدمها الطائرات.

بعض منصات الإطلاق مجهزة بنظام (اختياري) للتعرف على الطائرات الصديقة والمعادية ويعرف بـ IFF، وهو نظامُ اتصالاتٍ رقمية مشفرة يقوم بإرسال إشارة لاسلكية للطائرة يطلب فيها التعريف بهويتها ويقوم النظام الالكتروني للطائرة بالرد تلقائياً بإرسال إشارةٍ تدل على هويته. الاتصالات هنا مشفرة مما يعني أن الطائرة لا تستطيع الرد إلا إذا كانت تعرف شيفرة الاتصال، وفي حالة عدم الرد فهذا يعني أن الطائرة معادية ويتم استهدافها بالصاروخ.



رسم 7. مجال تغطية صاروخ أرض – جو قصير المدى و نسبة إصابته للهدف. هذا الرسم خاص بالطائرات المقاتلة التي تحلق بسرعة لا تقل عن 250 متر في الثانية. بالنسبة للطائرات المروحية فإن مجال التغطية يصبح دائرياً مما يعني أنه بالإمكان إسقاط المروحية في جميع الاتجاهات وفي مدى يصل إلى 4 كلم. إذا تم إطلاق الصاروخ على مروحية في مدى 1000–2000 متر فان الإصابة تكون مؤكدة و يعرف هذا المجال بمنطقة القتل.

يجب أن يطلق الصاروخ فقط إذا كان الهدف يحلق على ارتفاعٍ منخفض ويكون في ضمن مجال لا يزيد عن 4000 متر وارتفاعه يقل عن 3000 متر. احتمال إصابة الطائرة المقاتلة وهي تقترب أكبر بكثير من احتمال إصابتها وهي تبتعد، لأن الصاروخ قد لا يستطيع اللحاق بالهدف في حالة الطائرات المقاتلة العالية السرعة (رسم 7–8).

صاروخٌ واحد يدمر طائرةً ثمنها يزيد عن 30 مليون دولار أمريكي (السعر لا يشمل طاقم الطائرة !). عنصر المفاجأة عامل مهم في إسقاط الطائرة إذ أن بضعة ثوانٍ فقط تفصل إطلاق الصاروخ عن إصابته للهدف.





رسم **8**. أحد المجاهدين يضع قدمه على بقايا طائرة إف–16 بعد إسقاطها بصاروخ أرض– جو.
تم في نفس العملية إسقاط عدة مروحيات بلاك هوك من قبل مجاهدي دولة العراق الإسلامية بالتعاون مع جيش المجاهدين.

3. نظام التحكم الإلكتروني وملاحقة الهدف:

يستخدم صاروخ أرض – جو مجسات حرارية تعمل بالأشعة تحت الحمراء، هذه المجسات (اللواقط) تكون في هيئة كاميرا رقمية للتصوير الحراري تقوم بتصوير الجو والتقاط الصور الحرارية الصادرة عن محرك الطائرة الهدف، وتقوم بتتبع هدفها عن طريق ملاحقة مصدر الحرارة، بعض الصواريخ تستخدم أيضاً مجسات تعمل بالأشعة ما فوق البنفسجية لتمييز هدفٍ حقيقي عن هدفٍ وهمي. الأهداف الوهمية تكون عبارةً عن قنابل مضيئة تقوم الطائرات بإلقائها في حالة اكتشافها (بالرادار) لصاروخ موجه نحوها في وقتٍ مبكر من وصول الصاروخ إليها، هذه القنابل تصدر كمية عالية من الحرارة هدفها تحويل مسار الصاروخ لينفجر بعيداً عن الطائرة. الكاميرا الحرارية الرقمية مكونة من شبكة مجسات بقياس 2x2 في الأنواع القديمة، أو 128x128 في الأنواع الأحدث.

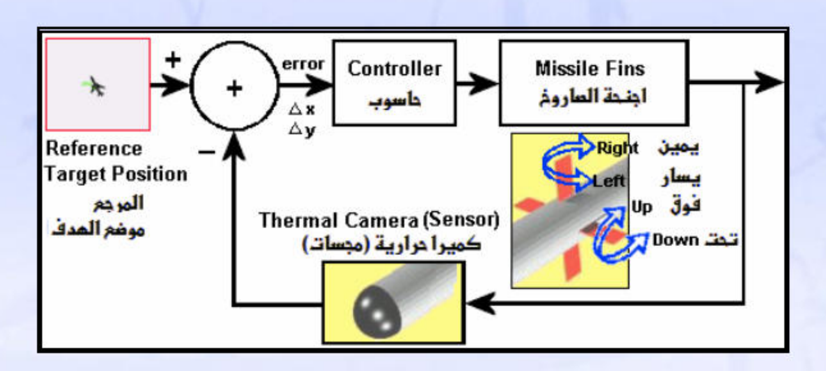
عند رصد الهدف يقوم النظام الإلكتروني للصاروخ بتحديد ما إذا كان الهدف داخل المجال الفعال، ويكون هذا بعد تصويب الصاروخ بحيث يكون الهدف في منتصف المنظار (رسم 9). وعندما يُصدر الصاروخ إشارة القفل مما يعني أن الباحث الحراري يقوم بتعقب الطائرة يتم إطلاق الصاروخ نحو الهدف.



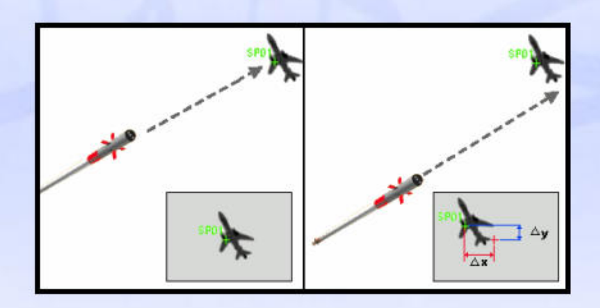
رسم **9**. طائرة نقل عسكري كما تراها كاميرا التصوير الحراري لصاروخ أرض – جو. الطائرة يمكن إسقاطها بسهولة. اللون الأسود يبين حرارة المحركات.



الصاروخ مجهَّزٌ بنظام تحكمٍ وقيادة آليّ مزود بحاسوب مدمج لمعالجة الصور الرقمية في زمـــن حقيقـــي (real time) (رســـم 10). الكاميرا ذات استشعار سلبي (passive) مما يعني أنها تستقبل الأشعة تحت الحمراء فقط ولا تقوم بإرسال أية أشعة. يحلق الصاروخ بسرعة عالية نحو الهدف ويقوم بالدوران حول نفسه بهدف استقرار الصاروخ أثناء الملاحة، وكونَ الهدف متحركاً أيضاً فإن الصورة الحرارية تبدأ بالإزاحة بعيداً عن مركز الصورة مما يعني أن الهدف ابتعد عن مسار الصاروخ، مما يجعل نظام التحكم يقوم بالتصحيح تلقائياً (رسم 11).



رسم **10**. مخطط نظام التحكم الآلي لصاروخ أرض – جو يعمل بالأشعة تحت الحمراء. يقوم نظام الملاحة بتحليل الصور الرقمية عن طريق وحدة معالجة رقمية ويتحكم بمحركات الأجنحة بحيث يحافظ على الهدف في مركز الصورة مما يعني أن الهدف في مسار الصاروخ الذي لا يستغرق سوى بضعة ثواني للوصول إليه وتفجيره.



رسم **11**. نظام التحكم و القيادة المدمج بالصاروخ يقوم بمعالجة الصور و تحديد نسبة إزاحة الهدف عن مسار الصاروخ ويقوم بتصحيح هذا الخطأ عن طريق تغيير اتجاه أجنحة الصاروخ لملاحقة الهدف وجعله دائماً في مركز الصورة. يسار الصورة: الطائرة على مسار الصاروخ تظهر في وسط صورة الكاميرا الحرارية للصاروخ. يمين الصورة: الطائرة تحركت نحو اليسار و تبدو الإزاحة واضحةً على مركز صورة الكاميرا الحرارية.

عندما يستعد المجاهد لإطلاق صاروخ يجب أن يكون الهدف واضحاً ويكونَ في مركز المنظار تقريباً. في حالة استهداف الطـــائرات المقاتلة (الفوق صوتية) فإن هذا الهدف يجب أن يكون محلقاً على ارتفاعٍ منخفض يقل عن 3000 متر وأن يكون في حالة اقتـــراب ولـــيس



ابتعاد، لأن الطائرة التي تبتعد لا يستطيع الصاروخ اللحاق بها إذا كانت سرعتها تزيد عن **250** م/ث (**900** كلـــم/ســـا). إضـــافةً إلى أن الطائرة يجب أن تكون ضمن المدى الفعال وهذا يعني أن تكون ظاهرةً بوضوحٍ في المنظار وأن لا يزيد بعدُها عن **4000** متر. قد تمر الطائرة جانبياً دون أن يستطيع المجاهد إسقاطها، وهذا لأن سرعتها تكون العامل الرئيسيّ في عدم إصابتها. بالنسبة لطائرات النقـــل أو الـــشحن العسكري بالإضافة للمروحيات فإن سرعتها بطيئة مما يسمح باستهدافها ضمن المدى الفعال دون النظر إلى كونها تقترب أو تبتعـــد، لأن سرعتها بطيئة نسبياً مقارنةً مع سرعة الصاروخ الذي قد يصل إلى ضعف سرعة الصوت، ولهذا فإن المجال الفعال يوجد داخل دائرة نصف قطرها يصل إلى **4000** متر (رسم **8**).

رغم أن مدى الصاروخ قد يصل إلى ضعف المدى الفعال فإنه لا يطلق إلا ضمن هذا المدى وذلك لسببين أساسيين: السبب الأول أن ملاحقة الصاروخ للهدف تعتمد على التقاطه نسبةً كافية من حرارة محرك الهدف، مما يعني أن الهدف يجب أن يكون واضحاً بـــشكله في منظار قاذفة الصاروخ قبل الإطلاق، والسبب الثاني أن الصاروخ بعد إطلاقه سوف يقطع مسافةً إضافية وهي المسافة التي ســـوف يحـــاول الهدف قطعها هروباً من الصاروخ. الوقود الصلب الذي يغذي المحرك يكفي فقط لقطع مسافة تتراوح بين **8000** و **10000** متر في معظـــم الأحيان.

4. الإجراءات المضادة:

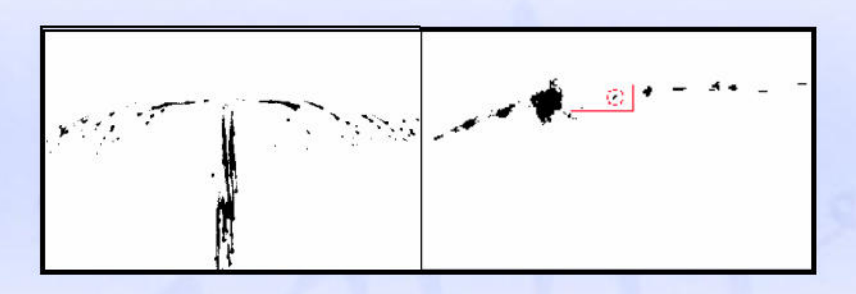
بعد إطلاق المروحية القنابلَ المضيئةَ (رسم **12**) ذات الحرارة العالية فإنها تستطيع الإفلات من صاروخٍ موجه بالأشعة تحت الحمراء. رغم هذا فإن هناك صواريخاً تستطيع التغلب على هذا الخداع.



رسم **12**. مروحية هجومية كوبرا تطلق قنابل مضيئة ذات حرارة عالية لمحاولة خداع وإبعاد صواريخ أرض – جو وصواريخ جو–جو التي تلاحق المصدر الحراري (يمين). طائرة شحن عسكري تحاول إبعاد صاروخٍ موجه حرارياً (يسار)



المربع الأحمر يوضح مكان المروحية والدائرة الحمراء تبين حرارة محرك المروحية، ونلاحظ أن القنابل المضيئة أصدرت طاقةً أعلى من محرك الطائرة (رسم 13). هذه الصور معكوسة الألوان – بلاك هوت (الأسود الساخن).

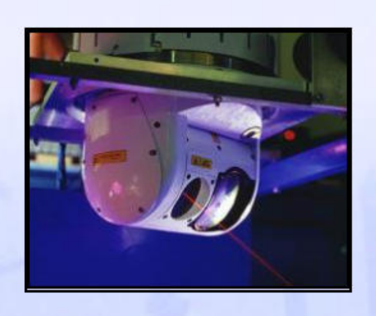


رسم 13. هكذا ترى كاميرا الصاروخ مروحية بلاك هوك في الرسم 9 (يمين) وطائرة الشحن العسكري (يسار). يتم التغلب عن هذه الإجراءات المضادة باستخدام صواريخ تستخدم مجسات بالأشعة فوق البنفسجية بالإضافة إلى المجسات الحرارية.

تصنع روسيا أنظمة دفاعٍ جويٍّ محمولة على الكتف (MANPADS) تستطيع التغلب على الإجراءات المضادة. سلسلة الصواريخ 9M32 (سام 7) تم التفوق عليها بنسخة معدلة عرفت بـ 9M34 ستريلا 3 (SA-14 غوملين)، والتي بدورها تم استبدالها بنظامٍ أكثر تطوراً وهو نظام إيغلا 9K38 أو SA-18 غروز، ونظام 9K310 ايغلا 1 أو نظام SA-16 غيملت. سلسلة الصواريخ إيغلا (IGLA) مزودة بباحث حراري مبرد بالنتروجين ثنائي الألوان ومزود برأس حربي زنته 2 كغ منها 390 غرام من المواد المتفجرة من نوع TNT، ويتميز بمقاومة عالية ضد القنابل المضيئة تمنحه القدرة على التعرف على الهدف الحقيقي بين الأهداف الوهمية، ويتم ذلك عن طريق مجساتٍ إضافية تعمل بالأشعة فوق البنفسجية، وهو يكافئ المواصفات التقنية لصاروخ ستنجر الأمريكي FIM-92 (جدول 1).

الصورة التالية (رسم 14) تبين أحدث نظامٍ تستخدمه الطائرات لإبعاد صاروخٍ موجهٍ نحوها بالأشعة تحت الحمراء. عندما يتم رصد صاروخ موجه نحو الطائرة باستخدام الرادار أو المجسات الحرارية فإنه يتم تفعيل نظام التشويش بالليزر حيث يقوم هذا النظام بتحديد مكان الصاروخ ليوجه نحوه حزمة ليزرية عالية الطاقة هدفها إتلاف الكاميرا الحرارية للصاروخ عن طريق تشبيعها بطاقة عالية، فإذا نجحت هذه المهمة فإن الصاروخ يفقد الرؤية ويقوم بتدمير نفسه تلقائياً بعد أن يفقد هدفه. لكن جميع هذه الإجراءات ليست فعالةً بنسبة عالية وخاصة بالنسبة للصواريخ قصيرة المدى، لأن الفارق الزمني بين إطلاق الصاروخ ووصوله لهدفه يقل عن خمسة ثواني في معظم الحالات، مما لا يدع فرصةً لقائد الطائرة باتخاذ إجراءاتٍ مضادة. بالإضافة إلى أن صواريخ حديثة مثل إس إي– 16 (SA-16) يحتوي على نظامٍ مضادٍّ للإجراءات المضادة، ولا تقلل هذه التقنيات الجديدة سوى نسبةً تتراوح بين 6% و 18% من احتمال إصابة الهدف.





رسم **14**. أحث تقنيات الإجراءات المضادة التي تستخدمها الطائرات لتجنب صواريخ أرض–جو الموجهة بالأشعة تحت الحمراء. بعد اكتشاف الصاروخ الموجه نحو الهدف يقوم جهاز ليزر بتوجيه حزمة حرارية عالية هدفها تشبيع الكاميرا الحرارية للصاروخ مما يعطلها و يبعد الصاروخ عن هدفه.

الخصائص/البلد المصنع	الولايات المتحدة الأمريكية	روسيا (الاتحاد السوفياتي سابقاً)		باكستان
اسم الصاروخ	ستنجر FIM-92C (series A,B,C,D,E,F)	SA-16 Gimlet (IGLA-1) SA-18 Grouse (IGLA)	SA-14 Gremlin (Strela 3- 9K34)	ANSA MK I,II,III
طول	**1.5** متر	**1.70** متر	**1.5** متر	**1.44** متر
أقصى مدى فعال	**4.8** كلم	**5.0** كلم	**4.1** كلم	**4.2** كلم إلى **15** كلم
أدنى مدى	**200** متر	**500** متر	**500** متر	**500** متر
أدنى ارتفاع	مستوى الأرض	**10** متر	**50** متر	**50** متر
المجسات الحرارية	تحت الحمراء – فوق بنفسجي	تحت الحمراء – فوق بنفسجي	تحت الحمراء	تحت الحمراء
أعلى ارتفاع	**3800** متر	**3500** متر	**3000** متر	**2300** متر
أقصى سرعة	**700** م/ث (**2.2** ماخ)	**600** م/ث (**1.8** ماخ)	**470** م/ث (**1.2** ماخ)	**500** م/ث (**1.47** ماخ)
الشحنة المتفجرة	**3.0** كغ	**2.0** – **3.0** كغ	**2.0** كغ	**1.0** كغ (**HE**)
ماخ= سرعة الصوت = **340** م/ث (على مستوى سطح البحر).				

جدول **1**. مقارنة بين أربع منظومات لصواريخ أرض– جو موجهة بالأشعة تحت الحمراء.





رسم **15**. فوق: صاروخ روسي الصنع إيغلا **9M39** مع القاذفة **9K38**، إس أي– **18** غروز (**SA-18 Grouse**). تحت: صاروخ روسي الصنع إيغلا **1 – 9M313**، مع القاذفة **9K310** ، إس إي– **16** غيملت (**SA-16 Gimlet**) و هو نسخة مصغرة من إس–**18** غروز.



رسم **16**. جندي يستعد لإطلاق صاروخ أرض– جو إس إي–**18** غروز (**SA-18 Grouse**).



5 الخلاصة:

في تقرير للاستخبارات الغربية فإن **500.000** صاروخ أرض– جو منتشرة عبر العالم ويستحيل التحكم في انتقالها، وفي إحصاءات حول استخدامها ذكرت مصادر غربية أن المجاهدين في أفغانستان إبان الاحتلال الروسي أسقطوا **269** طـائرة بـإطلاقهم **340** صـاروخ أرض– جو محمول على الكتف، وهذه الإحصاءات رغم محدودية الأرقام فيها فإنها دلالة واضحة على كفاءة هذه الأسلحة. أثناء حـرب الخليج الأولى أو ما عرف باسم "عاصفة الصحراء" استطاعت الصواريخ العراقية الموجهة بالأشعة تحت الحمراء إصـابة أهـدافها بنـسبة وصلت إلى **80%**، منها **56%** إصابات قاتلة، كما ذكرت التقارير الاستخباراتية أن هذه الصواريخ أثبتت كفاءةً عالية في إسقاط الطائرات المدنية بإصاباتٍ قاتلة وصلت نسبتها إلى **70%**.

في هذه الدراسة قمنا بالتعريف بالصواريخ أرض – جو المحمولة على الكتف وكيفية عملها وطريقة استخدامها بفعالية، سواء ضد الطائرات المقاتلة الفوق صوتية أو الطائرات المروحية وطائرات النقل أو الشحن العسكري ذات السرعات البطيئة. كما تطرقنا لأحـدث التقنيات التي تستخدمها الطائرات لمحاولة الإفلات من هذه الصواريخ والذي يعرف بالإجراءات المضادة، وبيّنّا تأثير هذه الإجراءات أمـام الصواريخ الذكية الحديثة والتي تستخدم التصوير الحراري مع مجسات بالأشعة فوق البنفسجية لمواجهة الإجراءات المضادة والتمييز بـين الهدف الحقيقي والهدف الوهمي.

كما نحب أن نبين لقارئنا الكريم أن المجاهدين أثبتوا بشكلٍ ملفتٍ للنظر براعتَهم في استخدام هذا السلاح والذي يكلف الاحتلال الأمريكي في العراق و أفغانستان خسائر فادحة، فصاروخٌ محمولٌ على الكتف يطلقه مجاهدٌ يمكن أن يسقط مروحية يزيد سعرها عن عشرة مليون دولار، أو طائرة بعشرات الملايين دون حساب ثمن الجنود الذين يقتلون في العملية !.

مصطلحات مهمة

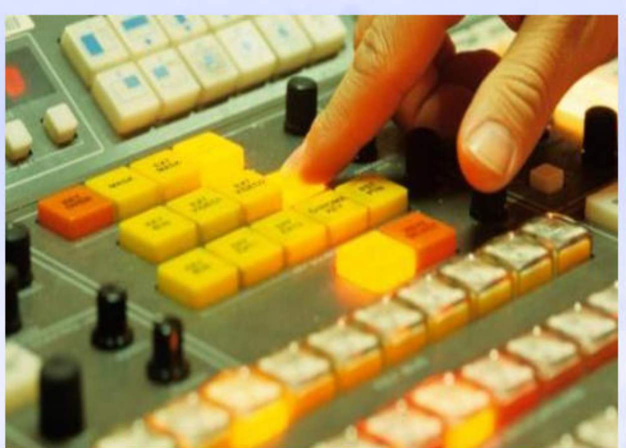
Missile	صاروخ
Short range	قصير المدى
Seeker	الباحث
Thermal	الحراري
Infrared (wavelength greater than 0.7 micron)	تحت الحمراء (طول موجة أكبر من **0.7** ميكرون)
Ultraviolet (UV: wavelength less than 0.4 micron)	فوق بنفسجي (طول موجة أصغر من **0.4** ميكرون)
Launch engine	محرك القذف
Rocket engine	محرك الصاروخ
Guidance	قيادة
Infrared seeker head	رأس الباحث بالأشعة تحت الحمراء
Explosives (High Explosive-HE)	متفجرات (شديدة الانفجار)

Launch tube	أنبوب القذف
Trigger	زناد
IFF (Identification Friend or Foe) antenna	هوائي نظام التعرف على الطائرات الصديقة و المعادية
Scope	منظار
Lock signal	إشارة القفل (الإقفال)
Altitude	ارتفاع
Navigation	ملاحة
Control	تحكم
Digital signal processing (DSP)	معالجة إشارة رقمية
Thermal image	صورة حرارية
Launcher unit	وحدة إطلاق
Incoming aircraft	طائرة قادمة
Coverage	تغطية
Launcher	قاذفة
Black hot	الأسود الساخن
Passive (signal receiver only)	سلبي (مستقبل إشارة فقط)
MANPADS (Man Portable Air Defense System)	نظام دفاع جوي محمول (على الكتف)
Supersonic	الفوق صوتية
Real time	الزمن الحقيقي
Counter-Countermeasures(CCM)	إجراءات مضادة للإجراءات المضادة
Directed infrared countermeasures [DIRCM]	إجراءات مضادة موجهة بالأشعة تحت الحمراء
Surface-to-Air Missile Systems (SAM)- Russia	أنظمة صواريخ أرض– جو (سام)– روسيا
Position tracking	تعقب الموضع
Sensors	مجسات (لواقط)
TNT Tri-Nitro-Toluene (explosive)	تي إن تي (متفجرات)
Fire and forget	أطلق وانسحب
Stability	استقرار
Micron (micro-meter)	ميكرون (ميكرو متر)
Sensor- Mercury Cadmium Telluride (HgCdTe) 1- 24µm	مجس خاص بالتقاط الإشعاع الحراري بين **1** و **24** ميكرون
Sensor- Indium Antimonide (InSb) 1- 5.5 µm	مجس خاص بالتقاط الإشعاع الحراري بين **1** و **5.5** ميكرون
ATAS (Air To Air Stinger)	ستنجر جو– جو
Kill zone	منطقة القتل



سلسلة الفيديو ـ سؤال وجواب (الجزء الثاني)

بقلم: مجاهد إعلامي



في هذه المقالة ما سنفعله هو التالي (إن شاء الله):

1- إضافة بعض المصطلحات إلى المقالة السابقة بحيث تكتمل جعبتنا منها إن شاء الله

2- سأتحدث عما يسمى بـــ معدل أخـــذ العينـــات (سأسميه معدل التعيين) sampling rate ، والدقة الأفقية size

3- معدل أخذ العينات العمودي والدقة العموديـــة (سيكون كسابقه تقريباً)

4- بعض المعلومات التقنية المزعجة عن أنواع برامج الالتقاط والفرق بينها بشكل عام

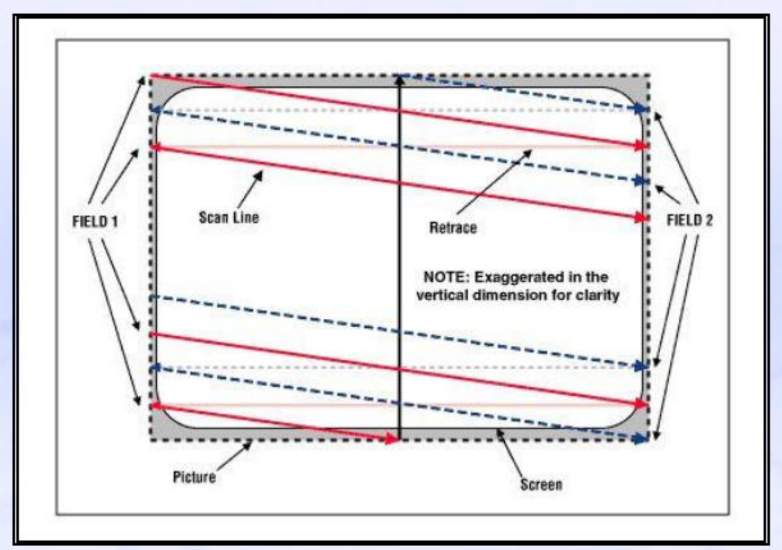
1. مصطلحات جديدة:

لنبدأ باستذكار بعض الأمور ..

الإشارة التلفزيونية تتألف –كما تحدثنا سابقاً– من خطوط زوجية (ستؤلف الحقل الزوجي) وخطوط فردية (ستؤلف الحقل الفردي) . هذه الخطوط تسمى بـــ خطوط المسح.

كما لاحظنا في صورة سابقة (وسأعيد تبيينه هنا) فإن حزمة الإلكترونات عندما ترحل من أيسر الشاشة إلى أيمنها لترسم خط مـــسح فإنها تعود إلى الجهة اليسرى لترسم الخط الجديد ، هذه العودة تسمى بالتراجع الأفقي horizontal retrace.





الحقول كما ذكرنا يتم إظهارها بتواتر 50 حقل في الثانية (PAL) و 59.94 حقل في الثانية (NTSC).

هذه الحقول مفصولة عن بعضها بما يسمى بـــ "الخطوط البينية الفارغة العمودية" وتكتب اختصاراً خطوط الـــ VBI (VBI lines) ، وهي لا تظهر على شاشة التلفزيون ، ولها وظيفة ولكنها لا تهمنا هنا ..

طيب إذن لماذا نذكرها طالما أن وظيفتها غير مهمة؟

نذكرها هنا لأن هذه الخطوط لا تحمل أي بيانات عن الصورة ، وإنما تحمل معلومات أخرى معروفة مسبقاً (من أجل التزامن وغيره).

ما مغزى هذا الكلام ؟ سواءً كانت تحمل معلومات معروفة أو غير معروفة .. فيم يهمني هذا الأمر؟

يهمنا أننا لا نحتاج إلى تخزين معلومات هذه الخطوط عندما نلتقط المادة المرئية التلفزيونية ، لأن معلوماتها معروفة مسبقاً .. فما يحدث هو أن جهاز أو كرت الالتقاط يقوم بإهمال هذه الخطوط (منقصاً حجم المادة المرئية الملتقطة) ، وعندما نقوم بتشغيل المـــادة المرئيـــة بعـــد الانتهاء منها على دي في دي مثلاً فإن مشغل الدي في دي يقوم بنفسه بإنشاء هذه الخطوط (لأنه كما قلنا يعرف ما تحتويه) !!

إذن هناك خطوط على الشاشة تحمل بيانات عن الصورة وخطوط لا تحمل ، فلنسمِّ هذه الخطوط التي تحمل البيانات **بالخطوط الفعالة active lines**.

هذه الطريقة في إظهار الصورة على التلفزيون (بوجود الحقول) تسمى –كما ذكرنا سابقاً– **بالتداخل interlacing** ، وكل الإشارات غير الرقمية تعمل بها.



قبل أن أستمر أريد فقط أن أقول أنه في الفقرة القادمة يوجد بعض الأرقام ، لا تهمنا بقدر ما تهمنا الفكرة العامة ..

إن خطاً من إشارة PAL يحتاج إلى 64 ميكرو ثانية (64 µs) ليتم رسمه من أيسر الشاشة إلى أيمنها. وهذا الخط يحمل بيانات عن الصورة ، ولكن ليس في كل مساره ، فمن هذه الــ 64 ميكرو ثانية يوجد حوالي 52 ميكرو ثانية تحمل معلومات الصورة ، وبقية الخط يحمل (كخطوط VBI مثلاً) معلومات معروفة مسبقاً تستخدم في المزامنة . فهذه أيضاً سيتم توفير مساحتها طالما أننا نعرف مسبقاً ما تحتويه.

وكما قلنا ، كل حقلين متتابعين سيشكلان صورة (أو إطارا) ، ونظام الــ PAL يعرض 25 إطاراً في الثانية (و 625 خط) ، ونظام NTSC يعرض 30 إطاراً في الثانية (و 525 خطاً) . علما أن الإختلاف الجوهري بين النظامين هو طريقة ترميز الألوان (Color encoding) حيث أنك إذا أدخلت إشارة فيديو من نوع NTSC على جهاز من نوع PAL فان الصورة تظهر بالأبيض و الأسود لأنه لا توافق بين طرق تعريف الألوان في كلا النظامين. و لكن هذا الأمر لا يسبب مشكلة لان الأجهزة الحديثة متعددة الأنظمة مما يعني أنها تستطيع التعرف على جميع طرق ترميز الألوان.

الآن معلومة قد تكون مفاجئة تقول أنه: في شاشة التلفزيون لا يوجد شيء اسمه بيكسل Pixel ، وإنما يوجد خطوط فقط ، لماذا ؟
لأن البيكسل هو شيء خاص بالإشارة الرقمية ، وإشارة التلفاز كما قلنا غير رقمية ، وبالتالي لا نستطيع أن نقول إن دقة شاشة تلفزيون ستكون كذا × كذا (كما في شاشة الحاسوب) ولكن عندما نريد أن نصف شاشة التلفزيون نقول أنها إما PAL (وبالتالي تحوي 625 خط) أو NTSC (وبالتالي تحوي 525 خط) ، وكل خط من هذه الخطوط يحتاج إلى 64 ميكرو ثانية ليتم رسمه كاملاً.

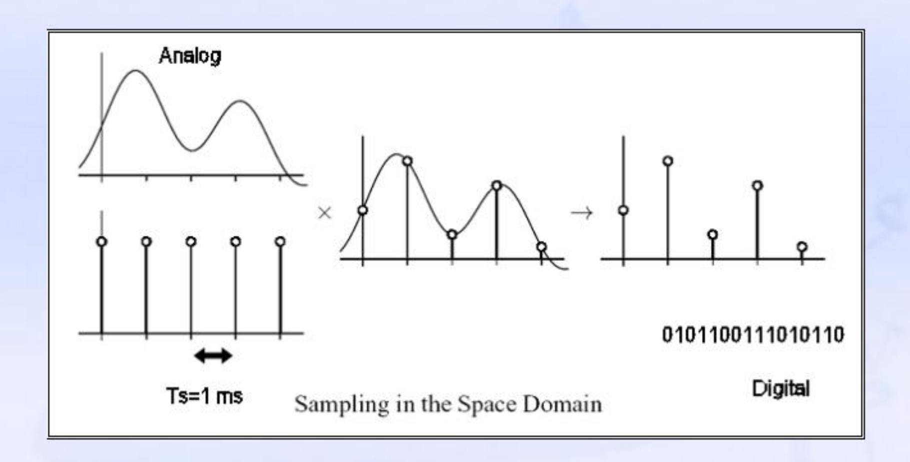
2. معدل أخذ العينات الأفقية:

ننتقل الآن إلى شيء جديد تماماً ، وهو الحديث عن معدل التعيين (أي أخذ العينات) Sample rate والدقة size :

كما قلنا في تعريف الالتقاط فإن مهمة جهاز الالتقاط هو تحويل الإشارة غير الرقمية إلى إشارة رقمية (ليفهمهـــا الحاســـوب) .. وكيف يقوم جهاز الالتقاط بهذه المهمة ؟ يقوم بها عن طريق ما يسمى بتقطيع الإشارة (أو أخذ العينات) signal sampling.
لنفهم معنى ذلك دعونا نتذكر أن الإشارة غير الرقمية (كإشارة الراديو) يتم رسمها على شكل موجات مرتفعة ومنخفضة (تسمى في الرياضيات موجات جيبية) ، والحاسوب لا يفهم هذه الإشارات ولكن ما يفهمه هو لغة الــ صفر والواحد 0/1 .. فكيف يمكننـــا أن نحول هذه الإشارة المستمر إلى أصفار وواحدات ؟
يتم ذلك بأن نحدد فترة زمنية قصيرة جداً (لنقل على سبيل المثال 1 ميلي ثانية) ، فيقوم جهاز الالتقاط كل (1 ميلـــي ثانيـــة) بقياس شدة الإشارة المستمرة ويسجلها (أي يأخذ عينة من الإشارة ويسجل شدتها كل 1 ميلي ثانية) ، وهكذا ففي حالة الــ 1 ميلي



ثانية فإن معدل حدوث أخذ العينات هذا هو **1000** مرة في الثانية (طالما أنه كل **1** ميلي ثانية يقوم بالقياس) ، وهذه الـــ **1000** مرة في الثانية هي ما نسميه بـــ **معدل أخذ العينة (وسأسميه معدل التعيين) sampling rate**. والصورة التالية توضح ما قصدت بكلامي :



Sampling in the Space Domain

ففي اليسار كانت الإشارة مستمرة ، تم تحديد فترات زمنية معينة يتم خلالها أخذ عينات من الإشارة لقياس شدتها ، ثم بعد ذلــك بقيت هذه القياسات على شكل أرقام متقطعة تحول إلى أصفار وواحدات (نظام ثنائي) يفهمه الحاسوب ، وهكذا ببساطة يتم تحويل الإشارة المستمرة غير الرقمية إلى إشارة متقطعة رقمية يفهمها الحاسوب . التحويل يمر بثلاث مراحل: **sampling, quantization, encoding**

في الحقيقة أنا أخذت مثالاً كل **1** ميلي ثانية مما نتج عنه معدل تعيين **1000** مرة في الثانية (أي **1000** هرتز) ، ولكن في الحقيقة فإن معدل التعيين يقاس بكذا مليون مرة في الثانية ، أي يقاس بالميغا هرتز **MHz**.

الآن أنت يا سيدي محظوظ جداً لأنك لا تقحم نفسك في كل هذه المشاكل ، كل ما تفعله هــو أنــك تــضبط برنــامج الــــ **VirtualVCR** (برنامج الالتقاط) على دقة صورة ولنقل **704x576** ، وتترك لكرت (أو جهاز) الالتقاط أن يقوم بكل التالي :

- أولاً يقوم جهاز الالتقاط بأخذ عينات بتواتر عالي (ليضمن أحسن دقة) .
- بعد ذلك يقوم بحذف خطوط الـــ **VBI** التي تكلمنا عنها .
- ثم سيحذف الخطوط الفارغة الأفقية (التي أيضاً لا تحمل بيانات عن الصورة) فيترك من كل خط حوالي (**52** µs) وهــو الجزء الذي يحتوي على بيانات الصورة.
- بعد ذلك سيستخدم العينات التي أخذها من هذا الجزء المتبقي ليوزعها على البيكسلات الأفقية (**704**) التي قام جنابــك بتحديدها مسبقاً.



- طبعاً لن ينسى أن يدمج الحقلين بحيث يقدم في النهاية صورةً دقتها كما طلبت تماماً 704x576 ، يقدم هذه الصورة الجاهزة إلى برنامج الالتقاط VirtualVCR ليفعل بها ما يشاء .
- وهكذا هذه هي وظيفة كرت (أو جهاز) الالتقاط ببساطة. ويستمر بعمله هذا إطاراً بعد إطار حتى ينتهي الفلم الذي تريده ويصبح جاهزاً وبشكل رقمي وبالحجم الذي طلبته لتقوم باستخدام برنامج VirtualVCR لتعديله ومعالجته كما تحب.

الآن دعونا نقوم بحسابات سريعة لما قمنا به :

قمنا بتوزيع µs 52 من إشارة التلفزيون على 704 بكسلات ، أي 704 التقاطة (التقاطة لكل بكسل) خلال 52µs ، فإذا قسمناهم سنجد أن معدل التقطيع هو: 704 عينة ÷ 52 ميكرو ثانية = 13.54 ميغا هرتز (13.54 MHz) ، وهذا هو معدل التعيين الحقيقي في حال طلبك لدقة 704x576. (طبعاً كما تلاحظ يختلف معدل التعيين باختلاف الدقة التي طلبتها فكلما زادت الدقة كلما احتاج الأمر إلى زيادة معدل التعيين) .

3. معدل أخذ العينات العمودية:

كل الإشارات المستمرة غير الرقمية في التلفزيون تنتج إما 576 خطاً فعالاً في نظام PAL أو 480 خطاً فعالاً في نظام NTSC . وكما قلنا فإن جهاز الالتقاط يقوم بتحويل الخطوط واحداً واحداً إلى بكسلات (كأنه يقسم الخط إلى أجزاء متساوية هي البكسلات المتراصة بجانب بعضها البعض أفقياً) . هذا الأمر يتم أفقياً .

أما عمودياً فالأمر أسهل بكثير فلا يوجد ما يمكن تقسيمه (لأن الخط يذهب أفقياً) ولكن توجد الخطوط نفسها المتراصة فوق بعضها ، فهذه الخطوط كل واحد منها يمكن اعتباره بكسل واحد .

وبالتالي لا تستطيع أن تتخير كثيراً في الدقة العمودية للشاشة ، فأمامك حلان (في نظام PAL مثلاً) إما أن تختار دقة عمودية 576 بكسل (على عدد الخطوط) أو أن تختار نصفها 288 بكسل (وفي الحالة الثانية كل ما على جهاز الالتقاط فعله هو أن يأخذ خطاً ويهمل آخر) .. وأي دقة عمودية تحاول اختيارها غير هذه ستؤدي إلى حدوث تشويه للصورة . أي أنك باختصار يمكنك أن تتحكم في الدقة الأفقية للصورة كما تحب وباختيارك هذا ستحدد لجهاز الالتقاط معدل التعيين ، أما في الدقة العمودية فلا تستطيع اللعب بها كثيراً وإنما تختار بين خيارين اثنين إما 576 أو 288 (في حالة PAL)

4. لمحة سريعة في برامج الالتقاط:

قبل أن نبدأ التطبيق العملي لعملية التقاط الفيديو بواسطة برنامج VirtualDub أو VirtualVCR علينا أن نجيب عن التساؤل التالي:

قد يقول أحدنا : "أرى أن هناك الكثير من برامج التقاط الفيديو ، مثل : VirtualVCR, iuVCR, VirtualDub, VirtualDubMod, AVIO, FLYDS وغيرها ، فأيها ينبغي أن أستخدم ؟"

في الحقيقة ، يمكنك أن تجربها جميعاً ثم تنتقي ما أعجبك وتخبرنا برأيك!، ولكن هناك بعض النقاط قبل ذلك قد توفر عليك الوقت:

- يوجد هناك نمطان من برامج قيادة أجهزة الالتقاط (device driver) : الأول يدعم موديل VfW وهو اختصار لـ (Video for Windows) ، والثاني يدعم موديل WDM وهو اختصار لـ (Windows Driver Model). وبناءً على ذلك فإن برامج الالتقاط تنقسم إلى قسمين :
  - القسم الأول يدعم WDM ، وهي تشمل : VirtualVCR , iuVCR و FLYDS.
  - القسم الثاني يدعم VfW ، وهي تشمل : VirtualDub, VirtualDubMod و AVIO.
- وبذلك نستنتج بالبديهة أن برنامج الالتقاط الذي ستستخدمه يعتمد على نوع جهاز قيادة بطاقة (أو جهاز) الالتقاط الذي تملكه .. فإن كان يدعم VfW فإنك تستخدم برامج مثل : VirtualDub, VirtualDubMod, AVIO . وإن كان يدعم WDM فإنك تستخدم برامج مثل VirtualVCR , iuVCR.
- طيب لا ينبغي لأي من الفريقين أن يقلق إن شاء الله لأننا سنشرح طريقة الالتقاط بكل من البرنامجين VirtualDub (والذي يدعم VfW) وVirtualVCR (والذي يدعم WDM).

طيب قبل أن تكمل ، ما رأيك لو تفضلت بإفهامنا شيئاً عن هذه الـ VfW و WDM ، فأنت لم تذكرها من قبل ..

حسن إذن، سنذكر الآن بعض المعلومات العامة حول كل من VfW و WDM .. ولكن بعض الإخوة قد يجد هذه المعلومات تقنية ولا تهمه أو لا يدري غايتها ، فإن وجدها تقنية زائدة عن اللزوم فليتجاهلها وليقفز إلى ما بعدها ولن يضره ذلك إن شاء الله ..

معلومات عامة عن VfW و WDM: (معلومات مزعجة أنصحك أن تتجاهلها تماماً)

- الـ VfW هو موديل برنامج قديم (ولا يتم تطويره حالياً) ، وبسبب حدوده الضيقة غير الموسعة جاءتنا مايكروسوفت بموديل برامج قيادة جديد وهو : WDM (بدأ مع ويندوز 2000).
- معظم برامج قيادة كروت الفيديو الآن يتم تطويرها باستخدام WDM .



- هناك برامج للتحويل بين VfW و WDM (تسمى بالإنكليزية wrapper)، وهي تسمح لك بأن تلتقط الفيديو باستخدام برنامج يدعم VfW (مثلاً VirtualDub) مع أن كرت الالتقاط عندك يدعم WDM. ولكنك ستحتاج إلى معالج سريع عند استخدام المحول (wrapper) لأنه سيؤدي إلى حمل كبير على المعالج.
- الـــ VfW ما زال مدعوماً في ويندوز 98 ، ويندوز 2000 ، ويندوز NT وويندوز XP ، ولكن المشكلة في معظم الأوقات هي في برنامج قيادة كرت الالتقاط ، فببساطة كروت الفيديو الجديدة لا تملك برامج قيادة VfW ، وفقط Hauppauge يملك برامج قيادة يدعم VfW من أجل W2K و XP .
- الـــ VfW لا يحتوي على مُوَلِّف تلفزيوني TvTuner ، في حين أن WDM يملك.
- إذا قمت بتحميل الـــ 9.0b DirectX (وكنت تملك PAL و W2K/XP) فكن متأكداً من أن تقوم بتحميل الباتش معه ، وإلا فإن مدخل التلفزيون عندك سيتوقف عن العمل.

لم أفهم شيئاً !!

طيب إليك المزيد إذن ☺!!

بعض المعلومات عن bt8x8 driver :

برامج قيادة كروت الفيديو الداعمة للـــ WDM من أجل الـــ bt8x8 chips منها :

1) **برنامج btwincap** : قد تواجه بعض المشاكل في التحميل والاستخدام ، الصوت يظهر كأنه مونو mono (بالمناسبة mono يعني الحالة التي يكون فيها الصوت الصادر عن كلا السماعتين في الكمبيوتر متطابق (لا تشعر بعمق الصوت و البعد الثالث). الـــ btwincap متوافق تماماً مـــع المحـــول (wrapper) لـــذلك يمكنـــك اســـتخدام btwincap-VirtualDub combo
2) **برنامج iulab tweaked wdm driver** : ولا يمكن استخدامه مع VirtualDub لأنه غير متوافـــق مـــع الـــ wrapper.

ملاحظات:

- ♥ الـــ Hauppauge driver هي برامج داعمة لـــ WDM و VfW والتي من المفترض أن تعمل تحـــت وينـــدوز 98 ، ويندوز 2000 ، ويندوز NT ، وويندوز XP (ولكنها لا تتيح لك الالتقاط بالحجم الكامل)
- ♥ الـ bt8x8 Chips : و هي عبارة عن معالج مسؤول عن التقاط الصور من المصادر التماثلية (الغير رقميـــة) analog مثل التلفاز أو جهاز إستقبال غير الرقمي و تحويلها إلى صيغة رقمية على الفور دون معالجة و انتظار . جميع أجهـــزة التقاط الفيديو أو التي تسمى video in تستخدم هذا النوع من المعالجات, و له نوعين معروفين (لا أذكر أرقامهمـــا الان) و لكن أحدهما يدعم استقبال FM و يدعم windows XP فقط و الآخر يدعم win98



صدقني لم أفهم شيئاً ولا أدري أصلاً لم تخبرني بكل هذا !!

أعلم أنك تجد المعلومات الأخيرة غريبة وغير مناسبة لسياق الكلام .. ولكن عندما نتقدم إن شاء الله في تقنيات الفيديو ستدرك قيمتها وأهميتها وسنضيف إليها إن شاء الله .. وعلى كل حال أبشركم بأن المعلومات التقنية المزعجة إنتهت والحمد لله.

5 خلاصة :

حتى هذه اللحظة شرحنا في هذه المقالة و المقالة السابقة الأساس النظري الذي سنحتاجه لفهم المراحل اللاحقة في هذه السلسلة حيث أنه ابتداء من العدد القادم ستكون هذه المقالة مليئة بالتطبيقات العملية التي تعتمد على ما تم شرحه حتى الآن.

مصطلحات مهمة

معدل التقطيع	Sampling frequency (rate)
التراجع الأفقي	horizontal retrace
الخطوط البينية الفارغة العمودية	VBI
الخطوط الفعالة	active lines
التداخل	interlacing
إشارة مستمرة	Continuous signal
إشارة متقطعة	Discrete signal
رقمية	Digital
نظام الفيديو التماثلي الأوروبي (هناك أيضاً نظام سيكام– SECAM)	PAL (European Analog video Format)
نظام الفيديو التماثلي الأمريكي و الياباني (نسختين 3.5 و 4.3)	NTSC (American-Japan Analog Video Format)
برامج قيادة العتاد في الحاسوب	Device drivers
التقاط	Acquisition
ترميز الألوان	Color encoding



ترجمة الأفلام من خلال العناوين الجانبية

بقلم: أبو الحسن المغربي

وُجدت العناوين الجانبية (Subtitles) من أجل إظهار ترجمة الأفلام بأي لغة دونما حاجة إلى التعامل مع برامج تحرير الفيديو, وهي عبارة عن ملف صغير يحتوي على نص الترجمة ومعلومات المزامنة يوضع بجوار ملف الفيلم الأساسي ويحمل نفس اسمه مع اختلاف اللاحقة, فإذا قام المستخدم بتشغيل الفيلم يقوم برنامج التشغيل بإظهار نص الترجمة آليا من الملف.



مثال لمقطع من فيلم "أبو الزبير المغربي" رحمه الله, ويظهر فيه العنوان الجانبي كما في الصورة (العنوان الجانبي هنا هو الجملة المكتوبة لا.. لا يا شمس ....)

1. مراحل إنشاء العناوين الجانبية:

عادةً فإن إنشاء العناوين الجانبية يمر بمرحلتين رئيستين:

- المرحلة الأولى: تحويل الكلام المنطوق في الفلم إلى نص مكتوب باللغة المطلوبة.
- المرحلة الثانية: تقطيع هذا النص –تبعًا للسياق وللمدة– إلى قطع صغيرة يتم مزامنتها مع محتوى الفيلم (أي ضبط توقيت بدء ظهور كل مقطع وتوقيت اختفائه).

تتم المرحلة الأولى وجزء التقطيع من المرحلة الثانية بشكل يدوي، أما مرحلة مزامنة المقاطع فيمكن لأجلها استخدام برنامج مساعد مثل: Subtitle Workshop

رابط التنزيل:
http://www.urusoft.net/downloads/subtitleworkshop251.zip

1.1 طريقة مزامنة المقاطع باستخدام برنامج subtitle workshop:

بعد فتح البرنامج عليك أن تنشئ ملف ترجمة جديد (من قائمة "ملف" اختر الأمر "ملف ترجمة جديد")، ثم عليك أن تحدد للبرنامج الفلمَ الذي تريد العمل عليه (من قائمة "فيلم" اختر الأمر "فتح").

الصورة التالية توضح شاشة البرنامج أثناء العمل على مزامنة المقاطع النصية لفلم "أبو الزبير المغربي" رحمه الله.



يمكن أن يتم التفريغ والمزامنة بطرق متعددة على حسب التفضيل، وهذا مثال لأحد هذه الطرق:

1. يتم تفريغ الفيلم إلى ملف نصي.
2. تقطيع التفريغ إلى مقاطع صغيرة، والأفضل أن يتم التقطيع أثناء مشاهدة الفيلم.
3. الذهاب إلى شاشة البرنامج وتشغيل الفيلم.
4. ضع إصبعك قريبة من زر Insert في لوحة المفاتيح وكلما استمعت إلى أول كلمة من بداية كل مقطع اضغط الزر Insert (هذه الخطوة من أجل إضافة مقطع جديد مزامَن البداية).
5. بعد الانتهاء من الخطوة الرابعة ستجد أن لديك مقاطع فارغة بعدد المقاطع التي في الملف النصي، ابدأ من البداية (من عند المقطع 1) وانقل كل مقطع من الملف النصي إلى البرنامج بالتتالي.
6. يجب عليك الآن أن تضبط مزامنة نهاية كل مقطع، وهذا يتم بالشكل التالي:
   أ. تأكد من أن الزر غير محدد لكي لا ينتقل إلى المقطع التالي تلقائياً.



ب. **حدد المقطع رقم 1.**

ج. **شغل الفيلم.**

د. **أثناء استماعك لآخر كلمة من المقطع الأول اضغط على الزر .**

هـ. **ستلاحظ أن البرنامج نقل التحديد إلى المقطع التالي.**

و. **كلما استمعت إلى آخر كلمة من كل مقطع اضغط الزر المذكور.**

7. **أعد مشاهدة الفيلم من خلال البرنامج وتأكد من عملية المزامنة لكل مقطع بداية ونهاية.**

بعد أن تنتهي من مزامنة الترجمة لكل المقاطع اختر من قائمة ملف الأمر "حفظ" وستظهر لك الشاشة التالية، اضغط على SubRip ضغطًا مُزدوجًا واحفظ الملف باسم مماثل لاسم الفيلم.



وهذا الذي نتج لدينا بعد الانتهاء من تفريغ ومزامنة النصوص وحفظ الملف:

zubair.mpg	65,491 ك.ب	ملف MPG
zubair.srt	4 ك.ب	ملف SRT

إذا انتهيت من إعداد العناوين الجانبية لأول لغة وضبط المزامنة يمكنك بعدها فتح الملف النصي باستخدام برنامج المفكرة وترجمة كل سطر إلى اللغة التي تريد دون المساس بالأرقام التي في بداية كل سطر (أو فوقه).

```
1
00:00:19,257 --> 00:00:24,661
ذهب ليطلبها... فقالت؛ أتعرف ماهي؟

2
00:00:26,387 --> 00:00:27,126
!قال نعم

3
00:00:28,641 --> 00:00:30,323
ومن ذا الذي لا يعرف مهرك؟

4
00:00:32,381 --> 00:00:33,341
يا مغنم العز

5
00:00:34,625 --> 00:00:35,180
يا درب الإباء
```

شكل يوضح جانبًا من ملف العناوين الجانبية بعد فتحه من خلال محرر نصوص.

مشاكل وحلول:

- ♥ التر جمة لا تظهر، بالرغم من وجود ملف الترجمة بجوار ملف الفيلم وبنفس الاسم.

سبب هذه المشكلة هو عدم وجود الإضافة الخاصة بعرض الترجمة في جهاز المستخدم. ولحل هذه المشكلة يتم تثبيت الإضافة المسماة **DirectVobSub** (الحجم 300 كيلو).

- ♥ الإضافة الخاصة بعرض الترجمة مثبتة في الجهاز لكن الترجمة لا تظهر مع الملفات من نوع **rm** و **rmvb** .

الحل هو بحفظ ملف الترجمة بصيغة **RealTime** (وليس **SubRip**).

2 خلاصة:

في هذا الموضوع تم شرح طريقة إنشاء ترجمات احترافية للأفلام الجهادية بحيث تظهر هذه الترجمة في أسفل الشاشة تماماً كما تشاهد على القنوات التلفزيونية. هذه الخاصية تساعد بشكل كبير في نشر الأفلام الجهادية بلغات متعددة وعلى نطاق واسع بين الناس .

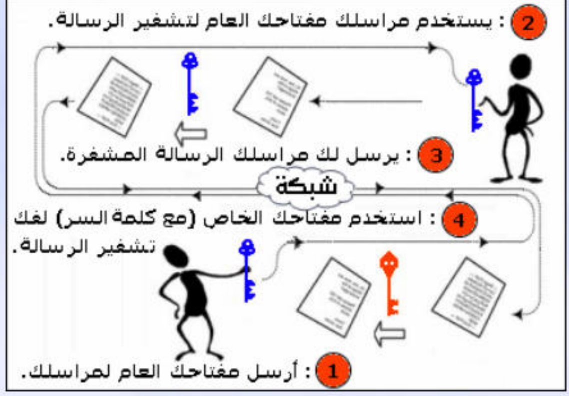
مصطلحات مهمة

العناوين الجانبية أو الترجمة بالمفهوم العام	Subtitles
إضافات يتم تركيبها في برامج تشغيل الفيديو أو غيرها لتعطيها ميزات إضافية	Plugins
إمتداد الملفات التي تعمل على برنامج real player	Rmvb, rm



برنامج أسرار المجاهدين: رؤية من الداخل

إعداد: القسم الأمني في الجبهة الإعلامية الإسلامية العالمية



برنامج أسرار المجاهدين هو أول برنامج إسلامي للتشفير اللامتناظر الخاص بالتراسل الآمن عبر الشبكات. البرنامج من إنتاج سرية الأمن التقني في الجبهة الإعلامية الإسلامية العالمية. يوفر هذا البرنامج إمكانية التراسل عبر برنامج آمن لأن البرامج الأجنبية الخاصة بأمن المعلومات غير موثوقة وليس من الحكمة استخدامها في حماية أسرار المجاهدين.

بعد ظهور ثغرات أمنية وشكوك كثيرة وقوية حول أشهر برنامج يقوم بتأمين الاتصالات الإلكترونية عبر الشبكات وهو برنامج بي جي بي (PGP) قامت الجبهة بإصدار برنامجها الخاص الذي يؤمن الاتصالات بأكبر قدر من السرِّية اعتماداً على أعلى المعايير التي توصَّل إليها علم التشفير وهندسة الاتصالات الرقمية. برنامج أسرار المجاهدين وجد ليوفر الاتصالات الآمنة لأنه يعتمد على كود مصدري قامت الجبهة بتطويره مستفيدين مما تم نشره من أبحاث لخوارزميات خضعت لتحاليل معمقة من أكبر العلماء و خبراء التشفير في العالم. وعلم التشفير يعامل على أنه سلاح الكتروني -وهو كذلك- لأنه أساسٌ في تأمين الاتصالات وضمان سلامة المتصلين وحماية أسرار المجاهدين. وليس هناك أخطر من أن يعتمد شخص على برنامج أجنبي لحماية أسراره وتأمين اتصالاته، فربما اكتشف بعد فوات الأوان أن جميع اتصالاته كانت مخترقة من قبل العدو. قال عمر بن الخطاب رضي الله عنه (لست بالخبِّ ولا الخبُّ يخدعني)، فأول الاحتياطات الأمنية أن تؤمِّن اتصالاتك ببرامج موثوقة.

وبرنامج أسرار المجاهدين يشبه في أهدافه برنامج PGP ولكن بميّزات جديدة وسرّية مفاتيح عالية. يتوفر برنامج أسرار المجاهدين بنسختين، نسخة أهل الثغور ونسخة أنصار الجهاد.

1. التشفير و التراسل عبر الشبكات:

التشفير هو وسيلة لحماية مراسلاتك ومعلوماتك من المتطفلين والجواسيس، وينقسم إلى قسمين: النوع الأول وهو التشفير المتناظر يستخدم مفتاحاً واحداً في التشفير وفك التشفير (كلمة السر)، وهو خاص بحماية المعلومات على الحواسيب بحيث لا تحتاج لنقل المفتاح أو كلمة السر، ومن أشهر الخوارزميات نذكر هنا (Rijndael, Mars, RC6, Serpent, Twofish). هذا النوع من التشفير غير صالح لنقل المعلومات المشفرة عبر الشبكات حيث لا يمكن نقل المفتاح أو كلمة السر، وهنا ظهر النوع الثاني من التشفير والمعروف باللامتناظر، ويعتمد على مفتاحين: المفتاح العام المخصص لعملية التشفير والمفتاح الخاص المستخدم في فك التشفير، ومن



أشهر الخوارزميات في هذا النوع RSA و ALG و هذا الأخير نسبة إلى مخترع الخوارزمية الدكتور طاهر الجمل، وتعتمد الخوارزمية على الخوارزم المتقطع. يتميز التشفير المتناظر بسرعته الفائقة بينما يعتبر التشفير اللامتناظر بطيئاً خاصةً بالنسبة لعملية فك التشفير، ولهذا فإن برامج الاتصالات عبر الشبكات مثل برنامج أسرار المجاهدين تستخدم كلا النوعين بحيث يتم استخدام التشفير المتناظر لحماية المعلومات ويتم استخدام التشفير اللامتناظر لحماية مفتاح التشفير المتناظر. ولمقارنة قوة المفاتيح بالنسبة لأنواع التشفير يكفي أن نذكر بأن مفتاحاً بطول 256 بت في خوارزمية متناظرة مثل AES يكافئ مفتاحاً بطول 15360 بت من نوع مفاتيح خوارزميات لامتناظرة مثل RSA.

بالنسبة لشبكات الاتصالات يعتبر البريد الالكتروني أحد أهم الوسائل الحديثة لتبادل الرسائل سواء كنت مشفرة أو غير مشفرة، ولضمان سلامة المسؤول عن الاتصالات يجب الالتزام بالشروط الآتية في التعامل مع البريد الذي يُستخدم لأمورٍ سرية:

1) عدم استخدام بريد الكتروني أمريكي (ياهو، هوتميل،....إلخ).
2) لا تستخدم أبداً بريدك الشخصي العادي وإنما قم بتجهيز بريد مخصص لتبادل الرسائل الحساسة.
3) عند حجز بريد للأمور الخاصة لا تدخل أية معلومة حقيقية بل قم بإعطاء معلومات وهمية (الاسم، العنوان، تاريخ الميلاد، الجنس، ....الخ).
4) عدم الدخول على بريدك الخاص من جهازك مباشرة بل يجب استخدام وكيل (بروكسي) للوصول لبريدك الخاص، بحيث حتى لو تمت متابعة بريدك فان رقم "آي بي" الذي تستخدمه لزيارة بريدك يكون رقماً بعيداً عن مكان اتصالك، لأن كل رقم "آي بي – IP" موجود في العالم مسجل في قواعد بيانات عالمية، ومعرفة الرقم الذي يستخدمه حاسوبك هو بمثابة معرفة عنوانك مباشرة، فالرقم يوصل للشركة المزودة للإنترنت والشركة توصل السائلين عنك إليك.

2. حول تشفير البريد الإلكتروني.

فيما يلي مقدمة تعريفية عن كيفية عمل نظام التشفير للرسائل: يعتمد نظام التشفير على خوارزمية التشفير بالمفتاح العام، وهذه الخوارزمية مبنية على تقنية تشفير تستخدم مفتاحين لإنجاز عملية التشفير: مفتاح عام ومفتاح خاص، المفتاح العام يستخدم في تشفير المعلومات فقط بينما المفتاح الخاص يستخدم في عملية فك التشفير، والمفتاحان معاً يشكلان ما يسمى حلقة مفتاح (Key-ring) لأن الحلقة لا تكتمل إلا بتوفر المفتاحين عند الشخص المعني.

2.1 قوة التشفير:

من أهم النقاط في قوة التشفير هو طول المفتاح والذي يحسب بالبت (Bits)، والتشفير المسموح به في بعض الدول هو 128 بت أو 256 بت في حالات نادرة (داخل الولايات المتحدة وكندا) بالنسبة للتشفير المتناظر (Symmetric)، أما بالنسبة للتشفير اللامتناظر (Asymmetric) فإن أمن المعلومات الحقيقي يتطلب مفتاحاً بطول لا يقل عن 1024 بت. يستحيل حالياً فك تشفير الرسائل المشفرة باستخدام المفاتيح الطويلة، ويكفي بأن نعرف أن مفتاحاً بطول 1024 بت في خوارزمية RSA (مفتاح مبني على أرقام بطول 309 رقم



عشري) يستحيل كسره حالياً حسب آخر ما توصل إليه علم الحاسوب وعلم حساب الأرقام الأولية (primes). وقد تطلب فك مفتاح 512 بت 5 أشهر من العمل المتواصل لـ 292 حاسوب متوازي فائق السرعة بحلول سنة 2000. ومفتاح 2048 أقوى من مفتاح 1024 بملايين المرات. وقوة المفاتيح تكمن أيضاً في ضمان إنتاجها (Key generation) بطريقة سليمة وليست مغشوشة، ولهذا السبب فإن استخدام برامج أجنبية يعتبر مجازفةً خطيرة حيث يمكن للشركات الأجنبية تصنيع برامج تنتج المفاتيح بطريقة تسمح لهم بالوصول للمفتاح الخاص اعتماداً على المفتاح العام.

2.2 المفتاح العام- Public key:

بعد أن تقوم بإنتاج مفتاح عام وآخر خاص وحماية المفتاح الخاص بجملة مرور "Passphrase" –كما سنوضح لاحقاً– يتم نشر المفتاح العام في مكان عام مثل المنتديات أو مواقع الإنترنت أو مزودات خاصة موجودة لهذا الغرض (servers)، وكل شخص يرغب في أن يرسل لك رسالةً مشفرة ما عليه إلا أخذُ مفتاحك العام وتشفير الرسالة باستخدامه ثم إرسالها إليك. الرسالة بعد تشفيرها لا يمكن فكُّها إلا باستخدام المفتاح الخاص، وهو سري ومتوفر عندك فقط، وبالتالي إذا أردت من شخصٍ أن يرسل لك معلومات مهمة فعليك أن ترسل له مفتاحك العام ليستخدمه في تشفير الرسالة قبل أن يرسلها إليك.

2.3 المفتاح الخاص - Private Key:

هذا مفتاح فك تشفير الرسائل التي تصلك والتي تم تشفيرها بالمفتاح العام. ويجب المحافظة على هذا المفتاح والاحتفاظ به في مكان آمن، كما يجب عمل نسخ منه مع المفتاح العام (حلقة المفتاح) ونسخها وتخزينها في مكان آمن، لأنه في حالة ضياع هذه المفاتيح فلا يمكنك بأي شكلٍ من الأشكال استرجاع البيانات أو الرسائل المشفرة باستخدامهما، وعليك إنتاج مفاتيح أخرى لاستخدامها مستقبلاً.

3. برنامج أسرار المجاهدين:

يقدم برنامج أسرار المجاهدين أعلى مستويات التشفير على الإطلاق في التشفير اللامتناظر الخاص بتبادل الرسائل والملفات بجميع أنواعها عبر الشبكات، وهو أول برنامج يوفر هذا النوع من التشفير من صناعة إسلامية بتشفير متناظر بطول 256 بت وبمفاتيح لامتناظرة بطول 2048 بت عالية السرية. البرنامج يدمج أعلى مستويات ضغط البيانات قبل تشفيرها لتصغير حجمها ويقوم باستخدام تقنية جديدة سُمِّيَت بالتشفير الشبح، وهذه الخاصية تمكن البرنامج من تغيير خوارزمية التشفير عشوائياً في كل مرة يتم فيها تشفير ملف وإنتاج مفتاح جلسة عشوائي يتغير في كل مرة، مما يسمح بالإفلات من محاولات تحليل الملفات المشفرة بحيث أن كل ملف يتم تشفيره بخوارزمية مختلفة من مجموع خمس خوارزميات يستخدمها البرنامج. أسرار المجاهدين يستخدم الخمس خوارزميات التي تم اختيارها من قبل خبراء التشفير في تصفيات اختيار خوارزمية "AES"، جميعها بمفاتيح بطول 256 بت.



تقنية التشفير اللامتناظر تسمح بنقل المفاتيح العامة عبر الشبكة، ويمكن نشر المفاتيح العامة في المنتديات الجهادية، وتستخدم بصمة المفتاح للتعرف على هوية جهة الاتصال، ويستخدم المفتاح العام في تشفير الملفات قبل إرسالها، والمفاتيح المستخدمة نفسها مشفرة لا يمكن استخدامها أو تحليلها ببرامج أخرى.



رسم **1**: الواجهة الرئيسية لبرنامج أسرار المجاهدين من إنتاج سرية الأمن التقني في الجبهة الإعلامية الإسلامية العالمية

4. مزايا البرنامج:

- التشفير باستخدام أفضل خمس خوارزميات في علم التشفير (**AES finalist algorithms**).
- مفاتيح تشفير متناظر بطول **256** بت (**Ultra Strong Symmetric Encryption**).
- مفاتيح تشفير لامتناظر **RSA** بطول **2048** بت (زوج مفتاح عام و خاص).
- ضغط بيانات مدمج (أعلى مستويات الضغط) (**Zlib compression**).
- مفاتيح و خوارزميات متغيرة بتقنية التشفير الشبح (**Stealthy Cipher**).
- التعرف التلقائي على خوارزمية التشفير أثناء فك التشفير (**Cipher Auto-detection**).



- تقنية المسح الآمن للملفات بحيث يتم مسح الملفات مع استحالة استرجاعها (**Files Shredder**).
- البرنامج مكون من ملف واحد لا يحتاج إلى تثبيت "**setup**" و يمكن تشغيله من ذاكرة محمولة "**Flash memory**".

5. إدارة المفاتيح:

عند تشغيل البرنامج لأول مرة ستكون قاعدة بيانات المفاتيح فارغة. اِضغط زر "إدارة المفـــاتيح **Keys manager**" ســـوف تحصل على النافذة التالية:

Keys Manager

Fingerprint:

Type	User ID	Key ID	Length	Creation

Key Management: Export Private Key... | Import Key... | Remove Key... | Export Public Key... | Generate Keys... | Change Passphrase...

No. Keys: No keys

Close

رسم 2: نافذة إدارة مفاتيح التشفير

اضغط على زر "إنتاج مفاتيح **Generate keys**" وسوف تحصل على النافذة التالية:

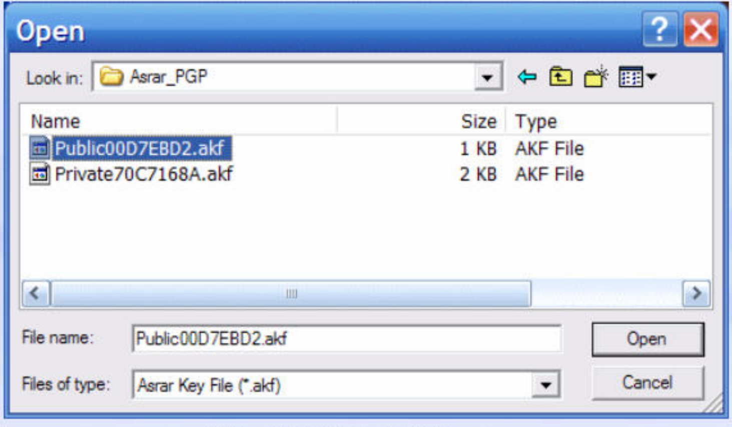


رسم 3: نافذة إنتاج زوج مفتاح جديد



قم بملء فراغات الاسم "Username" و جملة السر "Passphrase" وتأكيد جملة السر "Confirm Passphrase" ثم اضغط على زر "إنتاج الآن Generate Now". إذا كان جهازك يدعم اللغة العربية، يمكنك استخدام اللغة العربية في تعريف اسم المستخدم و جملة السر. اضغط على أزرار اتجاه الكتابة لاختيار لغة الكتابة (عربي – لاتيني). قد يستغرق إنتاج مفتاح 2048 بت فترةً تتراوح بين دقيقتين وخمسة دقائق على جهاز يعمل بسرعة 2.4 جيغاهرتز (2.4 مليار دورة في الثانية).

يكون البرنامج حين إنتاج المفاتيح مجمداً ويقوم باستغلال المعالج الدقيق "microprocessor" بنسبة 100%. بعد الانتهاء من إنتاج "زوج مفتاح Key pair" يمكنك إغلاق النافذة. تبين لك المعلومات في "الحالة Status" الفترة الزمنية التي استغرقها إنتاج المفاتيح. بعد انتهاء العملية يكون هناك ملفين جديدين وهما بشكل publicXXXXXXXX.akf و privateYYYYYYYY.akf، حيث يمثل الرقم XXXXXXXX رقم تعريف المفتاح العام (Key ID) و يمثل الرقم YYYYYYYY رقم تعريف المفتاح الخاص ويتم حفظهما في نفس مجلد البرنامج. يجب نسخ المفتاحين ونقلهما لمكان آمن (قرص مدمج أو ذاكرة محمولة... الخ) كنوعٍ من النسخ الاحتياطي، لأنه يستحيل استرجاع المعلومات المشفرة بالمفتاح العام من دون المفتاح الخاص. بعد إنتاج المفاتيح يمكنك تفعيلها عبر إدراجها بقاعدة بيانات المفاتيح الفعالة. قم بالضغط على زر "إدراج مفتاح Import key" وسوف تحصل على النافذة التالية.



رسم 4: نافذة إدراج المفاتيح الخاص والعام

قم بإدراج المفتاحين (العام والخاص) مرةً تلو الأخرى. عند إدراج المفتاح الخاص سوف يطلب منك البرنامج جملة السر "Passphrase" لأن كل مفتاحٍ خاص مشفر بجملة سرية خاصة به. بعد إدراج عدة مفاتيح يكون شكل نافذة "إدارة المفاتيح" كالتالي.





رسم 5: نافذة إدارة المفاتيح بعد إدراج عدة مفاتيح

تظهر المفاتيح العامة باللون الأزرق مع الشكل مفتاح أزرق بينما تظهر المفاتيح الخاصة باللون الزهري مبينة بشكل مفتاحين (أزرق و أحمر). يرمز المفتاح الأزرق للمفتاح العام بينما يرمز اللون الأحمر للمفتاح الخاص. يظهر المفتاح المختار حالياً **"Selected"** باللون الأصفر. المفاتيح التي يتم إدراجها تصبح فعالة في قاعدة البيانات الموجودة بالملف **"AsrarKeys.db"**. يمكن الاستغناء عن المفاتيح بعد دمجها في قاعدة البيانات ولكن يجب الحفاظ عليها في مكان آمن كنسخ احتياطية.

لإلغاء مفتاح من قاعدة البيانات (قائمة المفاتيح الفعالة) قم باختيار المفتاح المعين ثم اضغط على زر "إلغاء مفتاح **Remove key**". يتم إلغاء المفتاح من قاعدة البيانات وتبقى النسخة الأصلية التي تم إدراج المفتاح منها. عند اختيار مفتاح عام يمكن استخراج نسخة منه عن طريق الضغط على "استخراج مفتاح عام **Export Public Key...**". المفاتيح من **2048** بت آمنة لفترة تزيد على العشر سنوات، غير أن المفاتيح الحالية للبرنامج لا يمكن الحديث عن فترة صلاحية قصوى لها لأن المفاتيح مضغوطة ومشفرة لمنع حتى مجرد استخدامها في برامج أخرى. فيما يلي مثال عن ملف مفتاح عام بطول **2048** بت مشفر.

إذا حصلت على مفتاح عام بأحد المنتديات على شكل نص يمكنك نسخ المحتوى وحفظه في ملف بامتداد **".akf"** ثم استخدام إدارة المفاتيح في البرنامج (**Keys Manager**) لإدراجه في قاعدة بيانات المفاتيح عن طريق **"Import Key..."**.

#---Begin GIMF ASRAR El Moujahedeen 1.0 Public Key 2048 bit---
pyHAv5RbPuhWmwfeX+KjrJk9iHBjnCI1sKN8CqTbYZR3K6nqjk0hc1GXWnJ
U7QpiWLsgR6J+rsgSe8J5zJSh5oPCrzv2+K540q0MMwi8udJ5LpiWm20IoTy
ti0VrNxSXi0Mpohzc+pWOwMNDdaSKW1IOyXc+kd3ybFRJHXNXNUKPwDCn
/XPtSFNrWYj3vJVuBWn4VA7NTrOdzw2uTMJcNo3IGQA/hYDAOWY6bm+GZ
qL+61gXzLv52gg9X8Fxle9vleG+sSt8sjThHGWO2W0WNGP5imvMG0ZtGaM
eVvmEKdTKQxCW3Wmib0I4qLjYxXCEg/JgQosrMPuXd4Jf4VTQLQB37Yk5Ny
91oBgAm+mbNJjkl9Iko+mIAjD0MmjO+3niP/t19/Ezqb/+8EZvbriqmpBy2Jd
mm6CNTGX1PDLgGhPibTDnzL2WqghB7I34YX1ESXp/QXV7eKabdp6BkCqhw
8ZdDPcoLQzUbHswIRt8xcuSViHujCZ9Ds8OHhQqVizzXzCU1r1ApzWsiEu74cU
RAKCmqSbM2h1jGuSbastL/dUn/goxPGqTKjfvMg==
#---End GIMF ASRAR El Moujahedeen 1.0 Public Key 2048 bit----



عند اختيار مفتاح خاص يمكن استخراج نسخة جديدة منه أو استخراج المفتاح العام المرتبط به لأن المفتاح الخاص يحتوي على المفتاحين معاً (زوج مفتاح Key Pair). إذا قمت بإدراج مفتاحك الخاص فلا يوجد ضرورة لإدراج مفتاحك العام أيضاً حيث يتم استخدام الجزء العام منه للتشفير واستخدام الجزء الخاص لفك التشفير، بينما تظهر المفاتيح العامة فقط للجهات التي تقوم بمراسلتها. يمكن تغيير الجملة السرية التي تحمي مفتاحك الخاص و تحمي أيضا ملف "زوج المفتاح Key pair" عن طريق "تغيير جملة السر ... Change Passphrase". عندما تضغط على زر تغيير الجملة السرية للمفتاح الخاص تظهر لك النافذة التالية حيث يتم إدخال جملة السر الحالية وجملة السر الجديدة مع تأكيد الجملة السرية الجديدة، بعدها اضغط على "تطبيق التغيير Apply Change"، ثم أغلق النافذة لتعود إلى نافذة "إدارة المفاتيح".

Change Passphrase
User ID: Saif al Islam
Current Passphrase:
New Passphrase:
Confirm Passphrase:
Hide Typing
Apply Change | Clear | Cancel

رسم 6: كيفية تغيير كلمة السر التي تحمي المفتاح الخاص

بعد تغيير الجملة السرية لا تنس القيام باستخراج نسخة جديدة منه وحفظها باستخدام "Export Private key..."، ويتم استبدال الملف السابق بالملف الجديد بعد أن يطلب منك البرنامج تأكيد الاستبدال.



رسم 7: عند استخراج مفتاح من قاعدة البيانات، يتم التأكد إذا كان موجوداً على القرص قبل مسحه.

للحصول على معلومات مفتاح ما قم بالنقر المزدوج عليه "Double click". في حالة طلبت معلومات عن مفتاح عام فإن النافذة التالية تظهر لك حيث تبين الصورة أن المعلومات تتعلق بمفتاح عام وتظهر صورة مفتاح واحد.





رسم **8**: معلومات حول المفتاح العام

تستطيع الآن نسخ معلومات المفتاح بالنقر على زر "نسخ **Copy**" ولصق المعلومات في المكان الذي تريد، ويجب نشر هذه المعلومات مع مفتاحك، فالبصمة الرقمية للمفتاح هي التي تؤكد أنك صاحب مفتاح ما. ولكن يجب إيصال هذه المعلومات للجهة التي ترغب في التراسل معها بعدة طرق حتى تتأكد هذه الجهة أنك صاحب مفتاح عام معين. لمقارنة بصمة رقمية حصلت عليها مع بصمة المفتاح الحالي في إدارة المفاتيح قم باستخدام نافذة مقارنة البصمات بالنقر على الزر. قم بنسخ و لصق البصمة في مكان الإدخال **FPb**.



رسم **9**: مقارنة البصمة الرقمية للمفاتيح

تستطيع أيضاً تخزين معلومات المفتاح في صيغة ملف نصي بالنقر على زر "حفظ باسم ... **Save as**"(الرسم **8**).

في حالة طلبت معلومات عن مفتاح خاص فإن النافذة التالية تظهر لك، حيث تبين الصورة أن المعلومات تتعلق بمفتاح خاص وتظهر صورة زوج مفتاح (خاص وعام). انظر الصورة التالية:





رسم 10: معلومات حول المفتاح الخاص

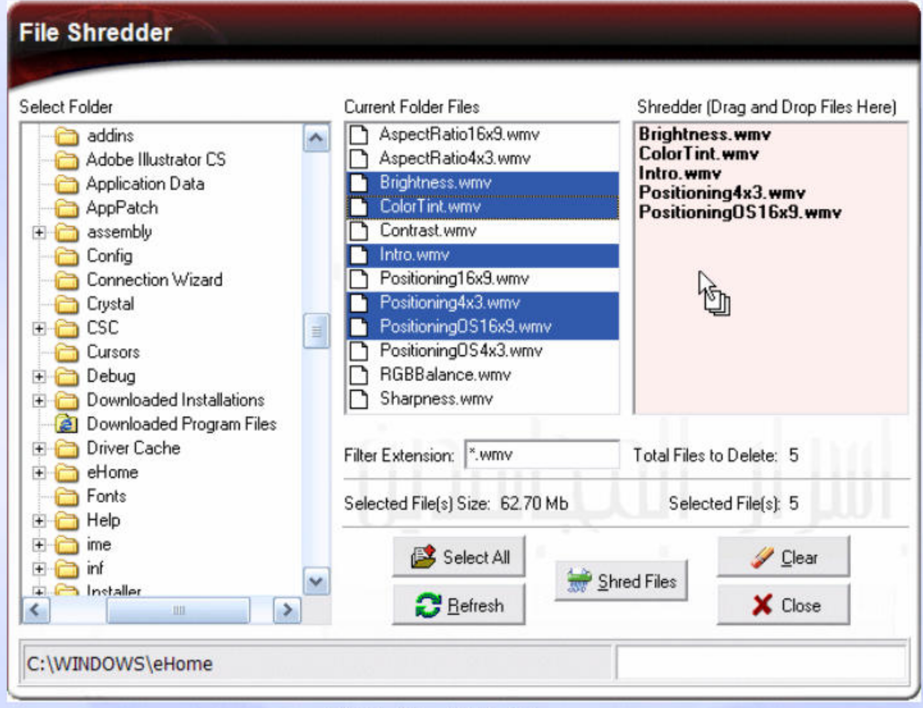
6. المسح الآمن للملفات:

لأن الملفات التي تتعامل معها لها طبيعة خاصة وتتطلب سرِّيةً تامةً في التعامل معها فإن البرنامج يوفر خاصية المسح الآمن للملفات التي تتعامل معها والموجودة على القرص الصلب لجهاز الحاسوب أو على ذاكرة محمولة. خاصية مسح الملفات التي يستخدمها نظام تشغيل الحاسوب ليست آمنة وذلك لإمكانية استرجاع الملفات التي قمت بمسحها باستخدام "Delete" وذلك باستعمال برامج خاصة معروفة باسم (Files Recovery)، وهذا يرجع لطبيعة عملية المسح الخاصة بنظام التشغيل الذي لا يقوم فعلياً بمسح الملفات وإنما بإلغاء تعريفها بالنظام ليسهل الكتابة في مكان وجودها على القرص مستقبلاً مما يسمح باسترجاعها في حالات كثيرة. عندما تتعامل مع ملفاتٍ سرّية يمكنك الاستفادة من خاصية المسح الآمن التي يوفرها برنامج أسرار المجاهدين حيث يقوم بعملية تدمير "Shredder" فعلي للملف، ويتم ذلك على مراحل تتراوح بين 4 و 10 مرات بطريقة تلقائية.

النافذة التالية تبين خدمة "تدمير الملفات". بعد أن تختار المجلد الذي توجد به الملفات تظهر هذه الأخيرة في قائمة الملفات الحالية "Current Folder Files". قم باختيار الملفات التي ترغب في تدميرها عن طريق الضغط على مفتاح "Ctrl" ثم انقر على كل ملف، بعد ذلك اسحبها بالفأرة "Drag and Drop" وضعها بداخل سلة الملفات المستهدفة بعملية التدمير. يمكن أيضاً أن تنقر نقراً مزدوجاً على كل ملف لنقله للسلة أو النقر المزدوج عليه داخل السلة للتراجع عن عملية إتلافه. لإتلاف جميع الملفات في مجلد معين اُنقر على زر " Select All". بعد الانتهاء من اختيار الملفات قم بالنقر على زر "تدمير الملفات Shred Files"، يقوم البرنامج بطلب تأكيد أخير على عملية الإتلاف بعدها يتم إتلاف الملفات نهائياً. لرؤية قائمة محدّثة للملفات اُنقر على زر "Refresh". للتراجع عن مسح ملفات قم بمسح قائمة الملفات داخل السلة وذلك بالنقر على "مسح Clear". تستطيع رؤية ملفاتٍ من نوع ما في قائمة الملفات الحالية باستخدام مرشح الملفات "Filter Extension" الذي يظهر الملفات التي تنتهي بامتداد معين. لإظهار جميع الملفات يتم استخدام الامتداد (*.*) في مرشح الملفات. أثناء إنجاز عملية تدمير الملفات يبين الشريط السفلي عملية التدمير (المسح الآمن) وعدد مرات المسح المستخدمة. يمكن تحديد عدد مرات المسح



الآمن في خصائص البرنامج "Options". كلما كان عدد المرات أكبر كلما كانت العملية أبطأ وخاصةً بالنسبة للملفات الكبيرة بينما لـــن تلاحظ الفرق بالنسبة للملفات الصغيرة (أقل من ميغابايت).



رسم 11: نافذة المسح الآمن للملفات

7. خصائص البرنامج:

7.1 ضغط البيانات:

يمكنك أن تختار نسب الضغط المستخدمة قبل التشفير. نسب الضغط العالية تتطلب بعض الوقت في معالجة البيانات (بضع ثـــوانٍ إضافية للضغط) بالنسبة للملفات الكبيرة (أكبر من 10 ميغا بايت)، بينما تكون سرعة الضغط فائقةً بالنسبة للملفات الصغيرة (أقل من 3 ميغابايت). وضغط البيانات مهم جداً خاصةً بالنسبة للملفات النصية (تقارير، رسائل، بيانات...إلخ)، وقد تصل نسب الضغط إلى أضعاف كثيرة. وتتراوح سرعة الضغط بين 10 و 100 ميغابايت في الثانية، ويوفر البرنامج أربعة خيارات: ضغط سريع، ضغط متوسط (عـــادي)، ضغط عالي (بطيء). كما تتوفر إمكانية تعطيل الضغط.

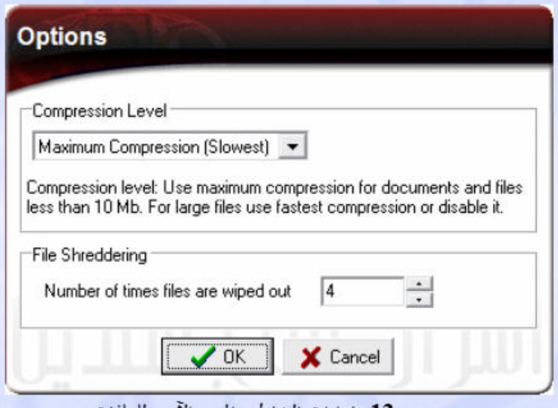
بينما يستحسن استخدام الضغط العالي في معظم الحالات، فإن إلغاء الضغط يكون مفضّلاً في حالة ملفات الفيديو الضخمة (أكبر من 50 ميغابايت) حيث أن الضغط لا يعطي سوى نسب قليلة، وذلك لأن طبيعة الملفات هي مضغوطة أصلاً. ونسبة الضغط تتراوح بـــين



0% بالنسبة للملفات المضغوطة و1000% بالنسبة للملفات النصية وبعض أنواع الصور، وقد تزيد كثيراً عن هذا (انظر مثال رسم 1 في أسفل الرسم).

7.2 إتلاف الملفات:

يتم هنا اختيار عدد مرات إتلاف (تدمير) الملف بحيث يستحيل استرجاعه، والخيارات المتاحة هي : 4، 6، 8 أو 10. عند تغيير الخصائص وحفظها بالنقر على زر موافق "OK" يتم إنشاء ملف خاص بالإعدادات الجديدة اسمه "asrar.ini". بالنقر على زر "إلغاء Cancel" يتم إهمال التغييرات الحالية. النافذة التالية توضح هذه الخصائص.

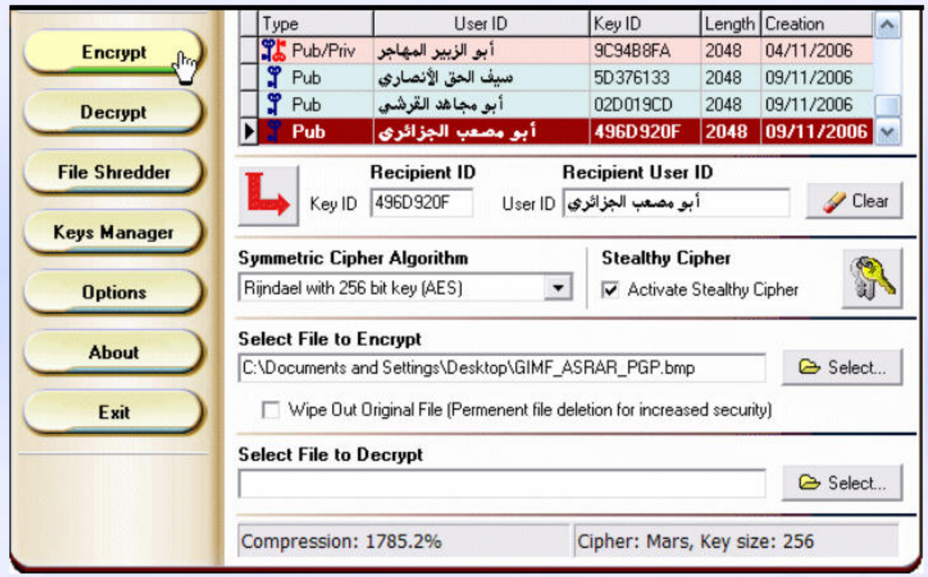


رسم 12: خيارات الضغط و المسح الآمن للملفات

8. تشفير الملفات بالمفتاح العام:

اختر الملف الذي ترغب بتشفيره "Select File to encrypt" ثم قم بالنقر المزدوج على المفتاح العام للجهة التي ترغب بمراسلتها، ويظهر المفتاح المختار في "اسم المستقبل Recipient User ID"، بعدها انقر على زر "تشفير Encrypt". عند النقر المزدوج على مفتاح يتحول لونه من الأصفر إلى الأحمر مما يبين أنه المفتاح الذي سوف يستخدم في التشفير.





رسم **13**: الواجهة الرئيسية توضح نسب ضغط عالية للبيانات

إذا اخترت "التشفير الشبح Stealthy Cipher" فإن خوارزمية التشفير يتم اختيارها تلقائياً بطريقة عشوائية، بينما يمكن تحديد خوارزمية التشفير من مجموع خمس خوارزميات إذا قمت بتعطيل خاصية "التشفير شبح Stealthy Cipher". إذا رغبت في إتلاف (المسح الآمن) للملف الأصلي بعد انتهاء عملية التشفير قم باختيار "Wipe Out Original File". إذا قمت باختيار هذه الخدمة عن طريق الخطأ فإن هناك فرصةً نهائية للتراجع حيث يطلب منك البرنامج تأكيد عملية إتلاف الملف الأصلي. بعد النقر على زر "تشفير Encrypt" تظهر نافذة تطلب منك الانتظار. والعملية تمر عبر ثلاث مراحل: الضغط والتشفير وأخيراً حفظ البيانات المشفرة. الملف المشفر يعطى نفس الاسم للملف الأصلي مع إضافة الامتداد ".enc"، ويتم حفظه في نفس مجلد الملف الأصلي. سرعة التشفير تزيد عموما عن 15 ميغابايت في الثانية. بعد تشفير ملف بالمفتاح العام فإنه يستحيل فك تشفيره من دون المفتاح الخاص.



رسم **14**: ضغط البيانات ثم تشفيرها و أخيراً تخزينها

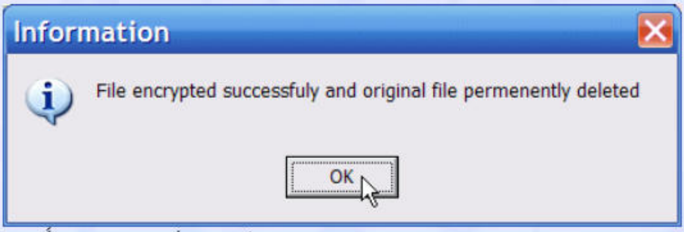


في نهاية العملية تظهر رسالة تخبرك بإنجاز عملية التشفير بنجاح.



رسم **15**: تبيان أن العملية تمت بنجاح

إذا طلبت إتلاف الملف الأصلي تلقائياً بعد تشفيره فإن الرسالة تكون التالية:



رسم **16**: نافذة إدارة المفاتيح بعد إدراج عدة مفاتيح وأن الملف الأصلي تم مسحه نهائياً.

9. فك التشفير للملفات بالمفتاح الخاص:

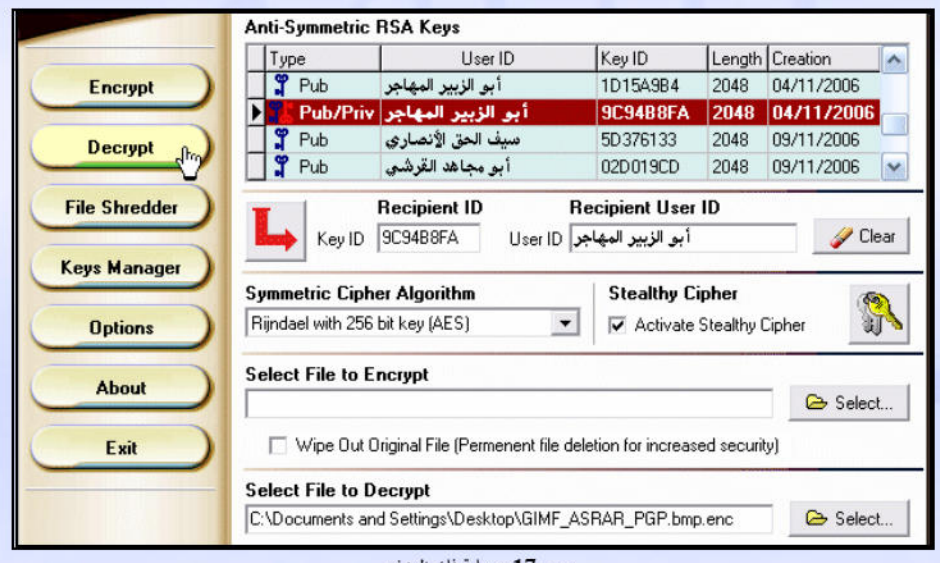
عندما يصلك ملف مشفر بمفتاحك العام المنشور بالمنتديات مثلاً فإنه بإمكانك فك تشفير الملف باستخدام المفتاح الخاص بك. قم باختيار الملف المشفر والذي ينتهي بالامتداد "enc.". قم باختيار المفتاح الخاص (Pub/Priv) بالنقر المزدوج عليه حيث يتحول لون المفتاح من الأصفر (لون المفتاح الحالي) إلى اللون الأحمر، ثم انقر على زر "فك التشفير Decrypt". يقوم البرنامج بطلب الجملة السرية الخاصة بالمفتاح الخاص لأنه من دون الجملة السرية يستحيل فك التشفير وذلك لكون المفتاح الخاص مشفراً باستخدام الجملة السرية "Passphrase". وحيث أن قوة التشفير تعتمد على خوارزمية من 256 بت فإنه يجب استخدام جملة سرية بطولٍ مكافئ لقوة التشفير وطول الجملة السرية يستحسن أن يتراوح بين 20 و 36 حرفاً.





رسم 17: عند فك تشفير ملف يطلب منك البرنامج كلمة السر التي تحمي المفتاح الخاص.

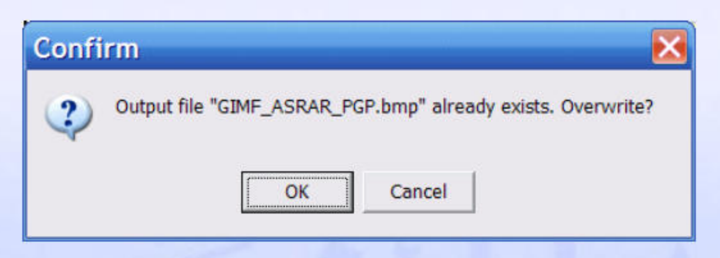
إذا قلَّ طولُ جملة السر عن الحد الأدنى تعرَّضَ مفتاحك الخاص للخطر إذا تمت سرقته من جهازك، والخطر الحقيقي على مفاتيحك هو نفسه الخطر الذي يهدد جهازك وهو برامج التجسس التي تُمَكِّنُ أصحابَها من اختراق جهازك المتصل بالإنترنت وسرقة ملفاتك.



رسم 17: عملية فك التشفير.

عند النقر على فك التشفير وكان هناك ملفٌّ بنفس الاسم على جهازك (في نفس المجلد) فإن البرنامج ينبهك لذلك ويطلب منك تأكيد استبدال الملف الذي يحمل نفس الاسم أو إلغاء العملية. في حالة لم ترغب باستبدال الملف قم بإلغاء العملية، بعد ذلك قم بتغيير اسم الملف المعني وأعد عملية فك التشفير مرة أخرى. وهذا موضح في الصورة التالية:

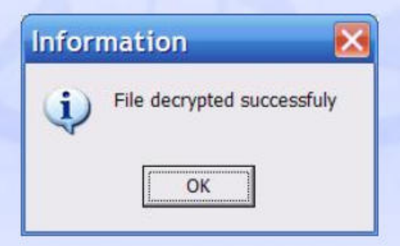




عند الاستمرار في فك التشفير فإن الرسالة التالية تطلب منك الانتظار. وعملية فك التشفير أطول زمنياً من عملية التشفير وتستغرق بضع ثوانٍ إضافية.



تحصل في النهاية على رسالة تبين نجاح عملية فك التشفير. إذا كان الملف المشفر لا يحمل الامتداد ".enc" فإن الملف الناتج سوف يحمل الامتداد ".dec" لتمييزه عن الملف المشفر. ولاستخدامه قم فقط بإزالة الامتداد ".dec" يدوياً.



10. ملفات البرنامج:

بعد تشغيل البرنامج يتم إنشاء ملفات إضافية:

1) ملف **AsrarKeys.db** : قاعدة بيانات مشفرة تحتوي على المفاتيح الفعالة بعد إدراجها في البرنامج. هذا الملف يتم إنشاؤه تلقائياً بعد التشغيل ويكون فارغاً حتى تقوم بإدراج المفاتيح بداخله عن طريق "**Keys Manager-> Import Key**".
2) ملف **asrar.ini** : ملف خيارات يتم إنشاؤه إذا قمت بتغيير الخيارات الافتراضية (**default settings**) ويتم حفظ الاختيارات الجديدة بداخله. إذا قمت بإلغائه يقوم البرنامج باستخدام الخيارات الافتراضية.



3) ملف المفتاح العام (publicXXXXXXXX.akf) وملف المفتاح الخاص (privateYYYYYYYY.akf)، وهذان الملفان يتم إنشاؤهما بعد عملية إنتاج زوج مفتاح جديد (Key Pair). عند إدراج المفتاح الخاص بالبرنامج ونشر الملف العام تصبح هذه المفاتيح احتياطية. ليس ضرورياً إدراج مفتاحك العام بداخل البرنامج لأن المفتاح الخاص يحتوي على نسخة من المفتاح العام.

لزيادة سرّية الملفات يمكنك تغيير أسماء المفاتيح والبرنامج ووضعهم في مجلد نظام التشغيل، ويفضّل أن تضعهم في ذاكرة محمولة صغيرة الحجم (القياسات) محميّة بكلمة سر يسهل إتلافها عند الحاجة.

11. خلاصة:

برنامج أسرار المجاهدين هو تقنية عالية في التشفير يفوق المستويات المعمول بها عالمياً في التشفير المتناظر ويوفر خاصية جديدة سميت بالتشفير الشبح باستخدام أفضل خمس خوارزميات في علم التشفير "Symmetric encryption". برنامج أسرار المجاهدين يحتوي على مزايا عديدة تجعله برنامج التشفير الوحيد الآمن للاستخدامات الجهادية. والبرنامج مكون من ملفٍ واحدٍ لا يتطلب التثبيت على الحاسوب ويمكن تشغيله من ذاكرة محمولة، كما يحتوي على خاصية المسح الآمن للملفات المصدر "مدمر الملفات File Shredder" أو ما يسمى الإتلاف النهائي للملفات الأصلية حيث يستحيل استرجاعها وتضمن بذلك سرية ملفاتك بعد مسحها إن شاء الله.

دعوة للمشاركة

أخي المجاهد التقني يامن تقرأ كلامي هذا

السلام عليكم و رحمة الله و بركاته

كم مرةً فكرت في خدمة هذا الدين ونصرة إخوانك المجاهدين إعلامياً ؟

هل تعتقد أن مجرد دخولك إلى المنتديات والقراءة فيها فقط بدون عمل يُعَدُّ خدمة لهذا الدين؟ متى ستنتقل أخي من مرحلة التلقي إلى مرحلة الإفادة؟

ألم يحن الوقت لأن تتفجر طاقاتك الكامنة وتصبح عضواً فاعلاً في الحرب الإعلامية بين المجاهدين وأعداء الله الصليبين؟

ألم تفكر يوماً أن لديك ما يمكن أن تنفع به إخوانك في دولة العراق الإسلامية الوليدة؟!!

أخي المجاهد التقني الكريم إن مجلة المجاهد التقني توفر لك هذه الفرصة، فما تملكه من علمٍ أخي هو أمانة يتعين عليك إيصالها إلى غيرك من المجاهدين ورواد المنتديات، فهذه المجلة سيطلع عليها عشرات الآلاف من الأشخاص سواء من المجاهدين أو أنصارهم في المنتديات وعامة المسلمين فيحصل لك بمقالتك الأجر العظيم.

أخي المجاهد التقني .. إن معركتنا مع أعداء الله الذين احتلوا ديارنا في فلسطين وأفغانستان والعراق والشيشان والصومال يدور نصفها على الأقل في الإعلام وتوعية المسلمين بحقيقة هذه الحرب الصليبية على المسلمين، ولقد كان هناك الكثير من النجاحات الهائلة للإعلام الجهادي التي شهد بها العدو قبل الصديق.

أخي المجاهد التقني .. بإمكانك اليوم البدءُ بإبداعاتك ومقالاتك العلمية التي تهم المجاهدين وأنصارهم من رواد المنتديات، ونحن نتكفل إن شاء الله بنشرها لكم في مجلتنا، فيصلُ ما تكتبه إلى عشرات الآلاف من القرّاء من إخوانك المسلمين الذين هم الآن في أمسِّ الحاجة لمثل هذه العلوم-وما نداء الشيخ أبي حمزة المهاجر حفظه الله عنا ببعيد-.

أخي المجاهد التقني الكريم .. ألم تسمع حديث رسول الله صلى الله عليه و سلم قال: ((إذَا مَاتَ الإِنْسَانُ انْقَطَعَ عَمَلُه إلاَ مِنْ ثلاثٍ: صَدَقَةٍ جَارِيَةٍ، وَعِلْمٍ يُنْتَفَعُ بِه، وَوَلَدٍ صَالِحٍ يَدْعُو لَه). أفلا تحب أن يبقى عملك هذا بعد موتك؟

أخي المجاهد التقني الكريم إن مقدار المسؤولية الملقاة عليك هي بقدر ما تملك من العلم، ولا تحقرنَّ أخي من المعروف شيئاً، فلعل مقالةً صغيرةً تكتبها فتُنشر لك هنا ينفع الله بها مجاهداً في سبيل الله أو تحمي بها أخاً لك في الله فيحصل لك بذلك الأجر العظيم إن شاء الله.

و نحن في هيئة تحرير المجلة يسرنا كثيراً رؤية ما تخطُّه أناملُكم من مقالاتٍ وإبداعاتٍ في خدمة هذا الدين العظيم. والمجالات التي نستقبل فيها المقالات إخواني واسعة وغير محصورة في علمٍ معين من العلوم التقنية، بل كل ما يفيد في الجانب التقني يمكن الإستفادة منه، وإن كنا في الأعداد الأولى نركز على الجانب الأمني الخاص بالشبكة العنكبوتية لأهميته القصوى للمجاهدين في سبيل الله ولأنه مسألة حياة أو موت بالنسبة لهم.

وفي الختام نسأل الله أن يوفقنا وإياكم لما فيه خير هذا الدين ونصره.

ملاحظات مهمة:
1) سيتم مراجعة أية مقالة مرسلة من قبل فريق من المتخصصين، وبعد إجازتها للنشر تُدَقَق ثم تنشر في المجلة.
2) المجلة تحرص على المقالات التي يتضح من خلال قراءتها أنه قد بذل فيها جهدٌ أصيلٌ ومميَز مدعَماً بالصور قدر الإمكان.
3) إن عدم نشر مقالتك في المجلة لا يعني بالضرورة أنها غير مناسبة ولكن قد لا يناسب طرحها لعدة أسباب تقدرها هيئة التحرير فيستفاد منها بشكل خاص وتمرر للعاملين في بقية الكتائب الإعلامية الجهادية.
4) عند إرسال أية مقالة الرجاء كتابة اسم مستعار أو كنية كاتب المقالة حتى تنشر بإسمه في المجلة.
5) يجب استخدام جميع أساليب التخفي الممكنة قدر الإمكان عند مراسلة المجلة فأعداء الله يتربصون بالمسلمين الدوائر.

6-ترسل المشاركات على العنوان التالي:

http://teqanymag.arabform.com

والسلام عليكم ورحمة الله وبركاته ...

أخوكم / رئيس التحرير
أبوالمثنى النجدي


المجاهد التقني
العدد الثاني لشهر صفر، سنة ١٤٢٨ هجرية
٢
قريبا
من مركز الفجر للاعلام :
لقاء مركز الفجر للاعلام بأحد القادة في أفغانستان . .
قريبا
في مجلة المجاهد التقني تقرؤون:
١ - المنتديات الجهادية و التصفح الامن
٢- الاسلحة الذكية: الرؤية الليلية و التصوير الحراري (الجزء الثاني)
٣ - جاسوس إسمه الهاتف الخلوي.
مركز الفجر للإعلام
الفجر